

# CT-6382D Wireless ADSL2/2+VoIP IAD User's Manual

Version A1.0, December 22, 2006

---



## **Preface**

This manual provides information to network administrators. It covers the installation, operation and applications of the IAD.

The reader reading this manual is presumed to have a basic understanding of telecommunications. For product update, new product release, manual revision, software upgrade, technical support, etc., visit Comtrend Corporation at <http://www.comtrend.com>

This document is subject to change without notice.



## **Warning**

- Before servicing this equipment, always disconnect all power and telephone lines from the device.
- Use an appropriate power supply and a UL Listed telephone line cord. Specification of the power supply is clearly stated in Appendix D - Specifications.

## **Copyright**

Copyright© 2006 Comtrend Corporation. All rights reserved. The information and messages contained herein are proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written permission by Comtrend Corporation.

## **Technical support**

When you find the product out of service, or that it doesn't work properly, please contact technical support engineer for immediate servicing or email to

[INT-support@comtrend.com](mailto:INT-support@comtrend.com)

# Table of Contents

|                  |  |           |
|------------------|--|-----------|
| <b>CHAPTER 1</b> | <b>INTRODUCTION .....</b>                                      | <b>5</b>  |
| 1.1              | FEATURES.....  | 5         |
| 1.2              | APPLICATION.....   | 6         |
| 1.3              | FRONT PANEL LED INDICATORS.....                                | 7         |
| 1.4              | SIDE PANEL .....   | 8         |
| <b>CHAPTER 2</b> | <b>INSTALLATION .....</b>                                      | <b>11</b> |
| 2.1              | HARDWARE INSTALLATION.....                                     | 11        |
| 2.2              | INSTALLING THE USB DRIVER .....                                | 13        |
| <b>CHAPTER 3</b> | <b>LOGIN VIA THE WEB BROWSER.....</b>                          | <b>18</b> |
| 3.1              | IP ADDRESS.....  | 18        |
| 3.2              | LOGIN PROCEDURE .....  | 20        |
| 3.3              | DEFAULT SETTINGS .....   | 21        |
| <b>CHAPTER 4</b> | <b>QUICK SETUP.....</b>  | <b>22</b> |
| 4.1              | WAN.....   | 24        |
| 4.2              | STATISTICS .....   | 25        |
| 4.2.1            | <i>LAN Statistics.....</i>                                     | <i>26</i> |
| 4.2.2            | <i>WAN Statistics.....</i>                                     | <i>27</i> |
| 4.2.3            | <i>ATM statistics .....</i>                                    | <i>28</i> |
| 4.2.4            | <i>ADSL Statistics .....</i>                                   | <i>30</i> |
| 4.2.5            | <i>Route.....</i>  | <i>32</i> |
| 4.2.6            | <i>ARP.....</i>  | <i>33</i> |
| 4.2.7            | <i>DHCP.....</i>   | <i>34</i> |
| <b>CHAPTER 5</b> | <b>QUICK SETUP.....</b>  | <b>35</b> |
| 5.1              | AUTO QUICK SETUP .....   | 36        |
| 5.2              | MANUAL QUICK SETUP .....                                       | 37        |
| 5.2.1            | <i>PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).....</i> | <i>39</i> |
| 5.2.2            | <i>MAC Encapsulation Routing (MER) .....</i>                   | <i>44</i> |
| 5.2.3            | <i>IP Over ATM.....</i>  | <i>48</i> |
| 5.2.4            | <i>Bridging.....</i>   | <i>52</i> |
| <b>CHAPTER 6</b> | <b>ADVANCED SETUP .....</b>                                    | <b>54</b> |
| 6.1              | WAN.....   | 56        |

|                  |                             |            |
|------------------|-----------------------------|------------|
| 6.2              | LAN.....                    | 57         |
| 6.3              | NAT.....                    | 58         |
| 6.3.1            | Virtual Servers.....        | 58         |
| 6.3.2            | Port Triggering.....        | 60         |
| 6.3.3            | DMZ Host.....               | 62         |
| 6.4              | SECURITY.....               | 63         |
| 6.4.1            | MAC Filtering.....          | 63         |
| 6.4.2            | Parental Control.....       | 65         |
| 6.4.3            | IP Filtering.....           | 67         |
| 6.5              | QUALITY OF SERVICE.....     | 70         |
| 6.6              | ROUTING.....                | 72         |
| 6.6.1            | Default Gateway.....        | 72         |
| 6.6.2            | Static Route.....           | 73         |
| 6.6.3            | RIP.....                    | 74         |
| 6.7              | DNS.....                    | 75         |
| 6.7.1            | DNS Server.....             | 75         |
| 6.7.2            | Dynamic DNS.....            | 76         |
| 6.8              | DSL.....                    | 78         |
| 6.9              | PRINT SERVER.....           | 79         |
| 6.10             | PORT MAPPING.....           | 80         |
| 6.11             | CERTIFICATE.....            | 83         |
| 6.11.1           | Local.....                  | 83         |
| 6.11.2           | Trusted CA.....             | 86         |
| <b>CHAPTER 7</b> | <b>WIRELESS.....</b>        | <b>87</b>  |
| 7.1              | WIRELESS BASIC SCREEN.....  | 87         |
| 7.1.1            | Security.....               | 89         |
| 7.1.2            | MAC Filter.....             | 92         |
| 7.1.3            | Wireless Bridge.....        | 94         |
| 7.1.4            | Advanced.....               | 95         |
| 7.1.5            | Quality of Service.....     | 99         |
| 7.1.6            | Station Info.....           | 100        |
| <b>CHAPTER 8</b> | <b>VOICE.....</b>           | <b>101</b> |
| 8.1              | SIP.....                    | 102        |
| 8.1.1            | Making Telephone Calls..... | 105        |
| 8.2              | DECT.....                   | 108        |
| <b>CHAPTER 9</b> | <b>DIAGNOSTICS.....</b>     | <b>109</b> |

|                    |   |            |
|--------------------|---|------------|
| <b>CHAPTER 10</b>  | <b>MANAGEMENT .....</b>                         | <b>111</b> |
| 10.1               | SETTINGS .....                                  | 111        |
| 10.1.1             | <i>Configuration Backup.....</i>                | <i>112</i> |
| 10.1.2             | <i>Configuration Restoration.....</i>           | <i>113</i> |
| 10.1.3             | <i>Restore Default.....</i>                     | <i>114</i> |
| 10.2               | SYSTEM LOG .....                                | 116        |
| 10.3               | TR-069 CLIENT.....                              | 118        |
| 10.4               | INTERNET TIME .....                             | 119        |
| 10.5               | ACCESS CONTROL .....                            | 120        |
| 10.5.1             | <i>Services.....</i>                            | <i>121</i> |
| 10.5.2             | <i>Access IP Addresses.....</i>                 | <i>122</i> |
| 10.5.3             | <i>Passwords.....</i>                           | <i>123</i> |
| 10.6               | UPDATE SOFTWARE.....                            | 124        |
| 10.7               | SAVE AND REBOOT .....                           | 125        |
| <b>TABLE A:</b>    | <b>ENCAPSULATION MODE – OPTIONS TABLE .....</b> | <b>126</b> |
| <b>APPENDIX A:</b> | <b>PRINTER SERVER CONFIGURATION .....</b>       | <b>127</b> |
| <b>APPENDIX B:</b> | <b>FIREWALL .....</b>                           | <b>133</b> |
| <b>APPENDIX C:</b> | <b>PIN ASSIGNMENTS.....</b>                     | <b>139</b> |
| <b>APPENDIX D:</b> | <b>SPECIFICATIONS.....</b>                      | <b>140</b> |
| <b>APPENDIX E:</b> | <b>SSH CLIENT.....</b>                          | <b>142</b> |

# Chapter 1 Introduction

Comtrend's CT-6382D is a powerful DECT Integrated Access Device (IAD), providing predictable, real-time, toll-quality voice over the Internet. The CT-6382D is for ADSL2/2+ over PSTN. It is designed for residential and business users who need to integrate ADSL2/2+, DECT, WLAN and VoIP technologies. With ADSL2/2+ broadband technology, the CT-6382D offers users easy access to the Internet via WLAN or Ethernet, and provides VoIP via standard analog phones.

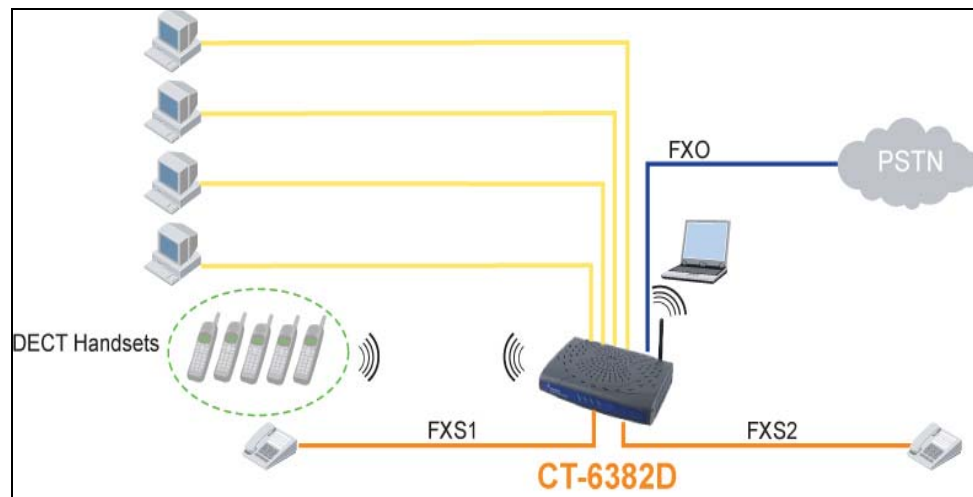
**Note:** All screenshots shown in this menu are based on the default setting, unless otherwise stated.

## 1.1 Features

- ADSL2/2+ VoIP and Router integrated
- Supports 2 DECT channels
- Integrated 802.11g AP (backward compatible with 802.11b)
- Supports life line: PSTN alive when power off
- Supports fast emergency call
- Supports Quality of Service (QoS) for voice
- Supports caller ID presentation and restriction
- Supports call hold
- Supports call waiting
- Supports call forwarding
- Supports call transfer
- Supports 3-way conference
- Supports Direct number dialing
- Remote administration and automatic remote firmware upgrade and configuration
- Supports VPN Pass-Through
- Supports parental control

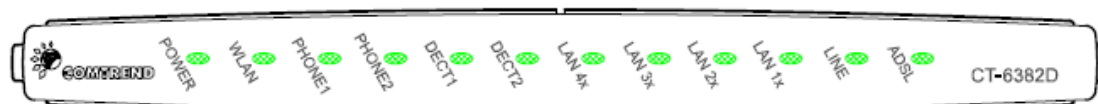
## 1.2 Application

The following diagram depicts the application of the CT-6382D.



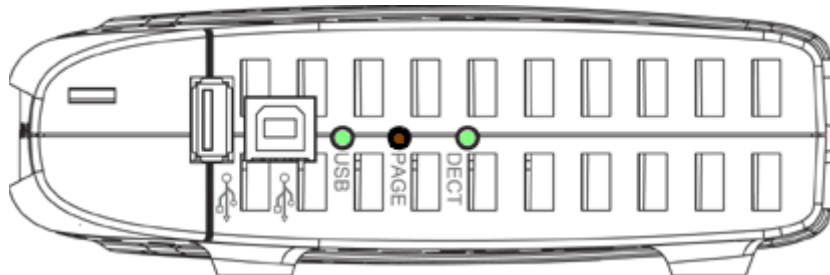
## 1.3 Front Panel LED Indicators

The front panel LEDs are shown in the picture below, followed by an explanation in the table below.



| LED                  | Color | Mode  | Function   |
|----------------------|-------|-------|--|
| <b>POWER</b>         | Green | On    | The VoIP IAD is powered up.  |
|                      |       | Off   | The VoIP IAD is powered down.                                      |
| <b>WLAN</b>          | Green | On    | The wireless module is ready.                                      |
|                      |       | Off   | The wireless module is not installed.                              |
|                      | Green | Blink | Data transmitting or receiving over WLAN.                          |
| <b>PHONE1</b>        | Green | On    | The FXS phone 1 is off hook.                                       |
|                      |       | Off   | The FXS phone 1 is on hook.  |
| <b>PHONE2</b>        | Green | On    | The FXS phone 2 is off hook.                                       |
|                      |       | Off   | The FXS phone 2 is on hook.  |
| <b>DECT1</b>         | Green | On    | DECT base truck line 1 in use                                      |
|                      |       | Off   | DECT base truck line 1 idle  |
| <b>DECT2</b>         | Green | On    | DECT base truck line 2 in use                                      |
|                      |       | Off   | DECT base truck line 2 idle  |
| <b>LAN<br/>4x~1x</b> | Green | On    | An Ethernet Link is established.                                   |
|                      |       | Off   | An Ethernet Link is not established.                               |
|                      | Green | Blink | Data transmitting or receiving over LAN.                           |
| <b>LINE</b>          | Green | On    | An FXO line is off hook.   |
|                      |       | Off   | An FXO line is on hook.  |
| <b>ADSL</b>          | Green | On    | The ADSL link is established.                                      |
|                      |       | Off   | The ADSL link is not established.                                  |
|                      | Green | Blink | The ADSL link is training or some traffic is passing through ADSL. |

## 1.4 Side Panel



|             |       |       |   |
|-------------|-------|-------|---|
| <b>USB</b>  | Green | On    | A USB link is established               |
|             |       | Off   | A USB link is not established           |
|             | Green | Blink | Data transmitting or receiving over USB |
| <b>DECT</b> | Green | On    | IAD is in registered mode for DECT      |
|             |       | Off   | IAD is not in registered mode for DECT  |
|             | Green | Blink | IAD is in paging mode for DECT          |

### Connection to USB port

Connect the USB port to a PC with a standard USB cable.

### Paging Function

Once registered, you can push the **PAGE** button (for one second) to locate the handset(s). To disable, simply push the **PAGE** button once again.

### Register Function

Hold down **PAGE** button for 10 seconds (You can also do this using the GUI interface by clicking on the Enable button\*.) Once DECT led illuminates use your DECT handset to register with the CT-6382D. Once the handset is registered the led will switch off and stop registered mode. Please note that if you don't register your handset(s) within three minutes, the register function will disable and the led will switch off.

\* Enable Register Mode

**COMTREN ADSL Router**

**Voice -- DECT configuration**

Enter the DECT parameters and click Apply to set DECT device.

|                  |         |
|------------------|---------|
| Dect HW Version: | 2       |
| Dect SW Version: | 8       |
| PIN Code:        | 0 7 2 3 |

|                     |      |
|---------------------|------|
| Dect Line 1 Status: | Idle |
| Dect Line 2 Status: | Idle |

Trunk Line 1 Gain Level: Tx: -13 dB Rx: +4 dB

Trunk Line 2 Gain Level: Tx: -13 dB Rx: +4 dB

Register Mode: Disable **Enable It**

| Phone No | Register state | Deregister               | Dect Line 1                         | Dect Line 2                         |
|----------|----------------|--------------------------|-------------------------------------|-------------------------------------|
| 1        | Empty          | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| 2        | Empty          | <input type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| 3        | Empty          | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| 4        | Empty          | <input type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| 5        | Empty          | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |

Apply Restore To Default

Once you have registered your DECT handset as shown below (based on the description given in your handset menu), if you want to deregister simply tick the deregister box and click **Apply**.

**COMTREN ADSL Router**

**Voice -- DECT configuration**

Enter the DECT parameters and click Apply to set DECT device.

|                  |         |
|------------------|---------|
| Dect HW Version: | 2       |
| Dect SW Version: | 8       |
| PIN Code:        | 0 7 2 3 |

|                     |      |
|---------------------|------|
| Dect Line 1 Status: | Idle |
| Dect Line 2 Status: | Idle |

Trunk Line 1 Gain Level: Tx: 0 dB Rx: 0 dB

Trunk Line 2 Gain Level: Tx: 0 dB Rx: 0 dB

Register Mode: Disable **Enable It**

| Phone No | Register state | Deregister                          | Dect Line 1                         | Dect Line 2                         |
|----------|----------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 1        | Registered     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| 2        | Empty          | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| 3        | Empty          | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| 4        | Empty          | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| 5        | Empty          | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |

Apply Restore To Default

Clicking Restore To Default you restore all the default settings as well as deregistering all handsets.

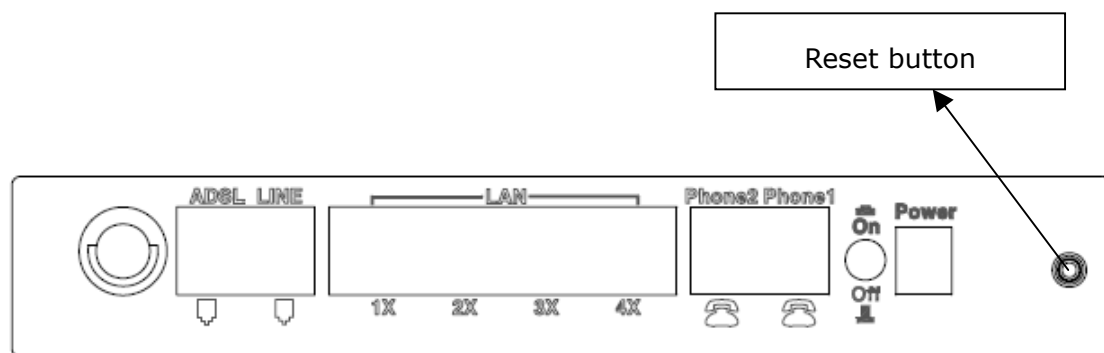
We can reach 5 Dect handsets however only two Dect handsets can be used at one time. Therefore we need to assign which phone can use which line to make/receive calls. For example, above we mapped Dect line 1 to Dect phones 1,3,5 and Dect line 2 to phones 2,4.

Please Reference the SIP section assign which SIP account to Dect Line 1 and Dect Line 2.

## Chapter 2 Installation

### 2.1 Hardware Installation

In the rear panel, there is a reset button. To load the factory default settings, hold the reset button down for at least 5 seconds. If held down for more than 12 seconds, the VoIP IAD will go into firmware update state and the user can update the VoIP IAD from web-interface @192.168.1.1 without ID/Password.



Follow the instructions below to complete the hardware connections.

#### Connection to ADSL port

Connect the ADSL line to the ADSL port with a RJ11 connection cable.

#### Connection to LAN port

To connect to a hub or PC, use a RJ45 cable. You can connect the VoIP IAD to up to four LAN devices. The ports are auto-sensing MDI/X and either straight-through cable or crossover cable can be used.

Connect the telephone set to the RJ11 **Phone1/ Phone2 port** for VoIP service.

### **Connection to Power**

Connect the **Power** jack to the shipped power cord. Attach the power adapter to the wall outlet or other AC source.

After all connections have been made, push the power-switch in to the on position. After power on, the VoIP IAD performs a self-test. Wait for a few seconds until the test is finished, then the VoIP IAD will be ready to operate.

Note: Restore the default parameters of the VoIP IAD by holding down the device's Reset button until the LED's start blinking simultaneously (about 5 seconds). After the device has rebooted successfully, and if the connection is established, the LAN LED, ADSL LED will display in green, depending on the connection type.

---

**Caution 1:** If the VoIP IAD fails to power up, or it malfunctions, first verify that the power supply is connected correctly. Then power it on again. If the problem persists, contact our technical support engineers.

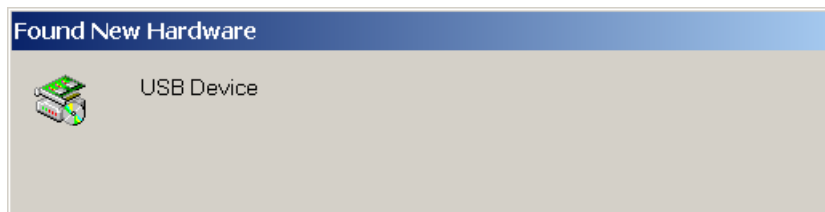
**Caution 2:** Before servicing or disassembling this equipment always disconnect all power cords and telephone lines from the wall outlet.

## 2.2 Installing the USB Driver

Before you connect your VoIP IAD's USB cable to your PC, you must load the ADSL USB drivers. The USB driver supports Windows 98, ME, 2000, and XP.

To connect the VoIP IAD to a PC using the USB interface, you need to use a standard USB cable and install the USB interface software. Follow the steps below:

**STEP 1:** Connect the USB VoIP IAD to the PC by plugging the flat connector of a standard USB cable into your PC, and plugging the square connector into the VoIP IAD. The screen will display as below:

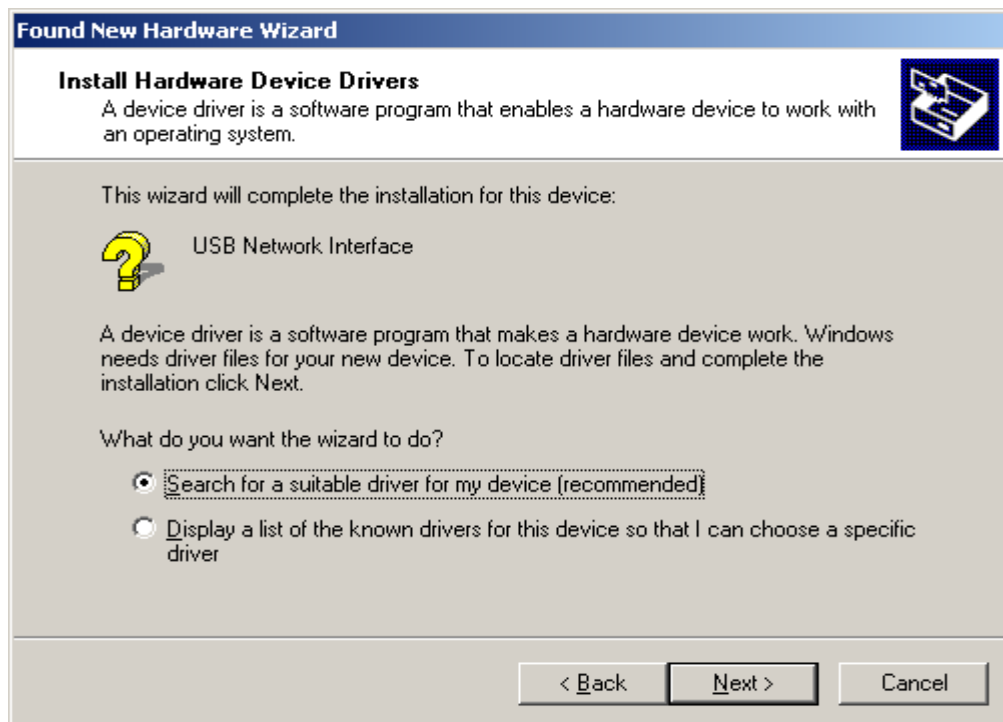


**STEP 2:** When the screen displays as below, click the **Next** button.

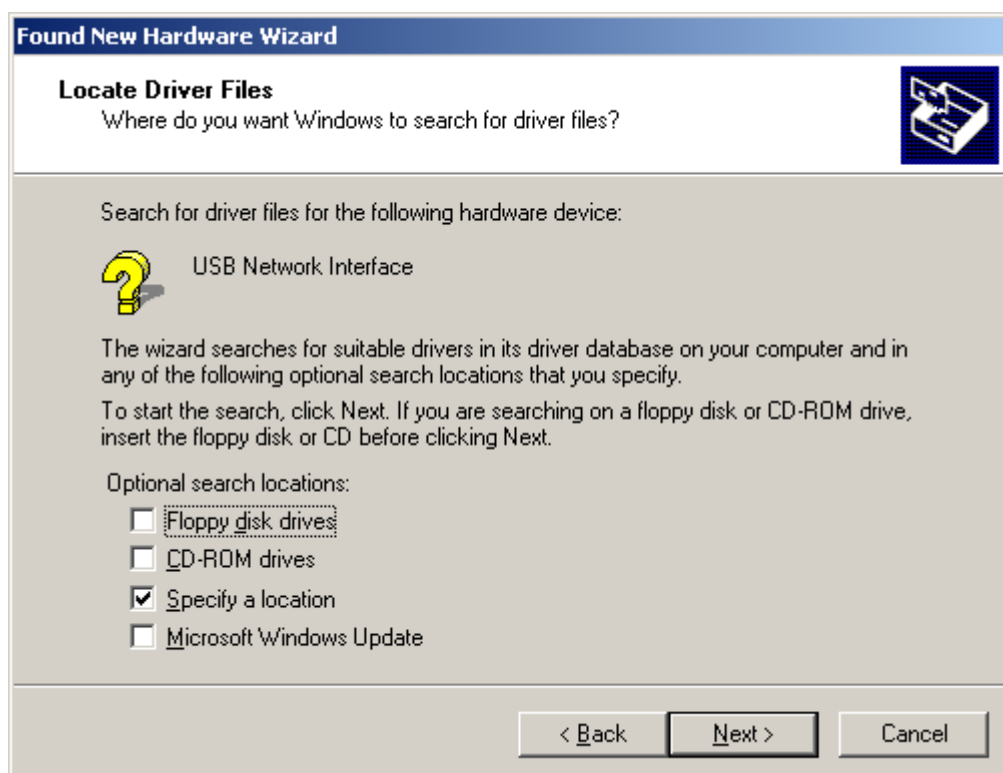


**Note:** This screen won't be displayed if the USB Driver has been previously un/installed.

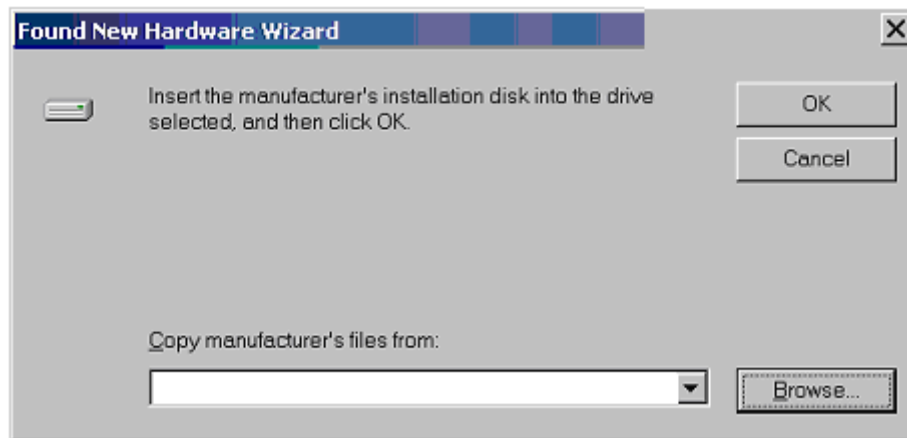
**STEP 3:** When the screen displays as below, select **Search for a suitable driver** and click the **Next** button.



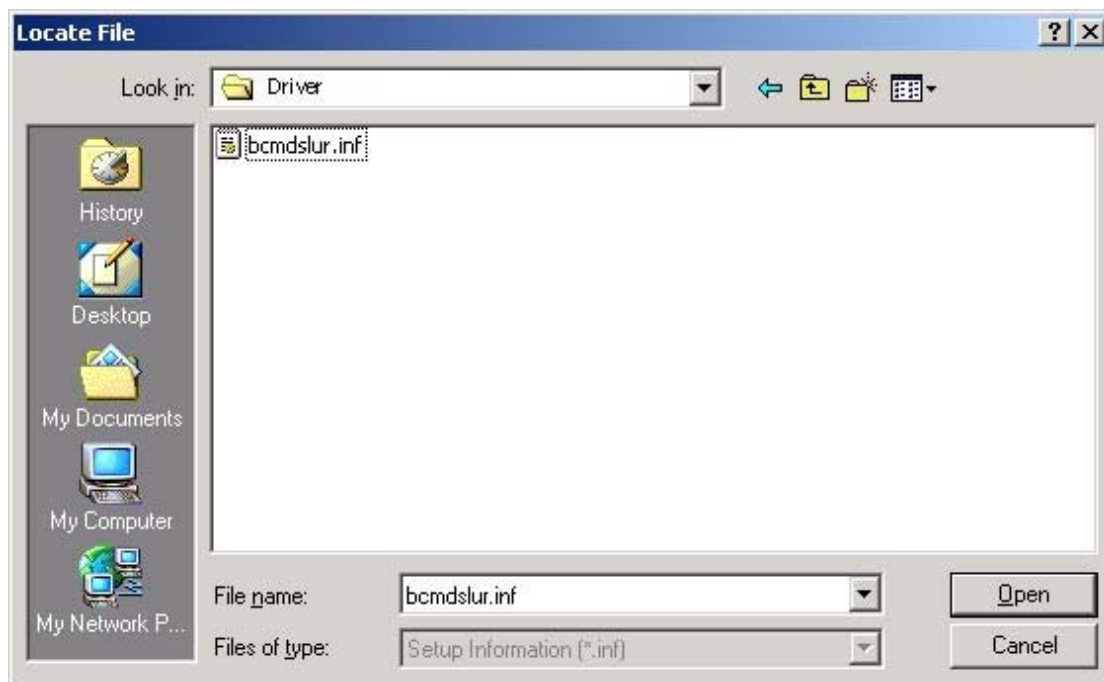
**STEP 4:** Select Specify a location and click the Next button. If you are installing the software from a disk, insert the disk.



**STEP 5:** Select the location of the file using the **Browse** button. Normally, the file is on the CD-ROM shipped with the device.



**STEP 6:** Locate the file, and push the **Open** button.



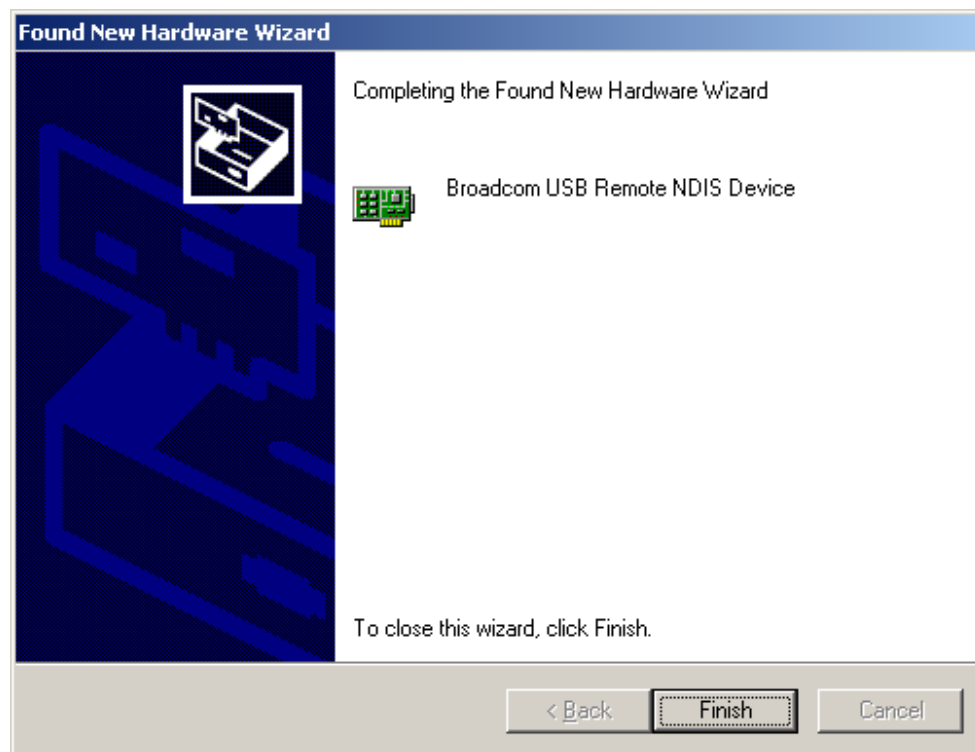
**STEP 7:** When the screen displays as below, push the **OK** button.



**STEP 8:** When the screen below displays, push the **NEXT** button.



**STEP 9:** Click the **Finish** button, when the screen displays as below.



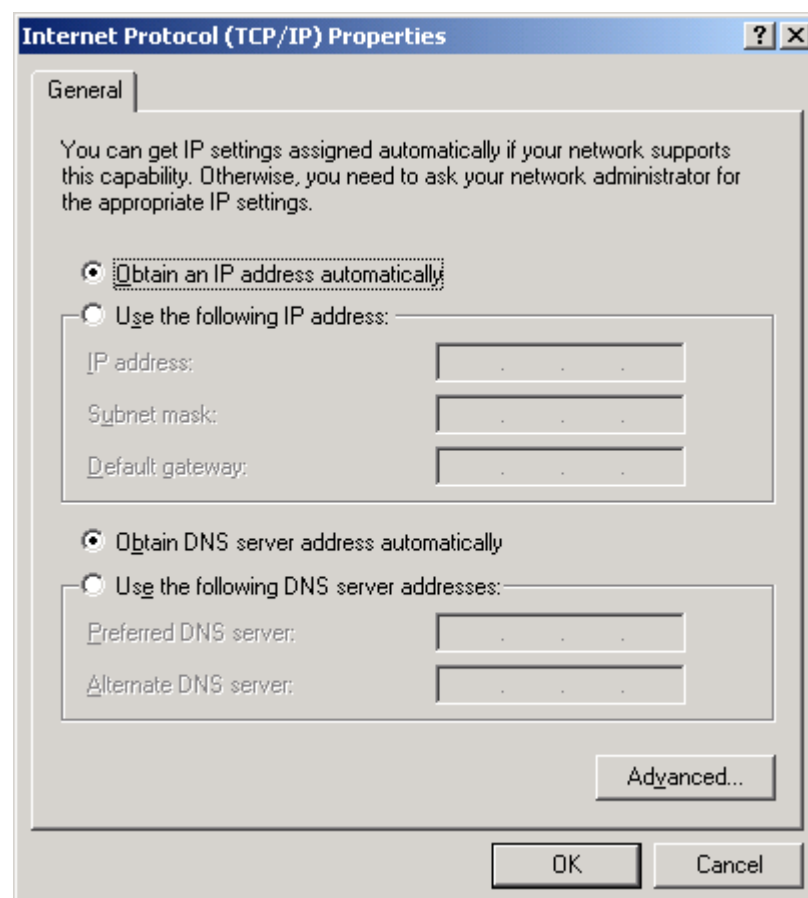
**STEP 10:** Installation is complete.

## Chapter 3 Login via the Web Browser

This section describes how to manage the VoIP IAD via a Web browser via the remote end. You can use a web browser such as Microsoft Internet Explorer, or Netscape Navigator. (The Web page is best viewed with Microsoft Internet Explorer 5.0 and later): A unique default user account is assigned with user name **root** and password **12345**. The user can change the default password later when logged in to the device.

### 3.1 IP Address

**Note:** When the CT-6382D is switched on, the DHCP server will start automatically. The default address for the CT-6382D is 192.168.1.1 and DHCP is enabled as default for the PC. You can automatically obtain an IP by selecting Obtain an IP address automatically, as shown here:

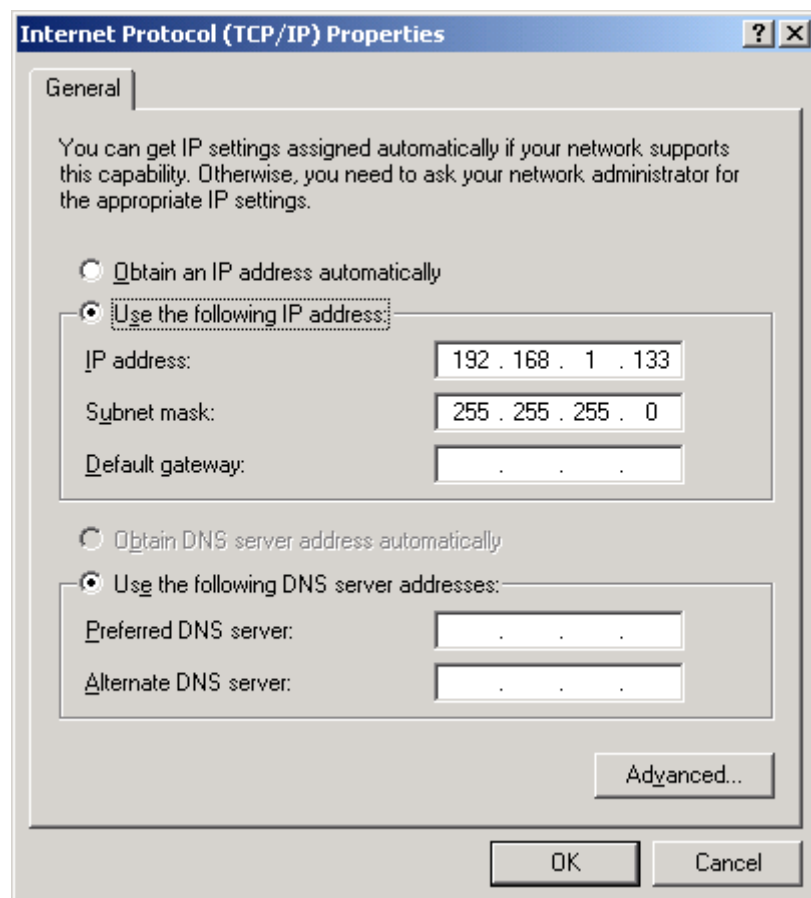


Shown below for your reference is the manual method.

The default IP address of the CT-6382D (LAN port) is 192.168.1.1. To configure the CT-6382D for the first time, the configuration PC must have a static IP address within the 192.168.1.x subnet. Follow the steps below to configure your PC IP address to use subnet 192.168.1.x.

**STEP 1:** Right click on the Local Area Connection under the Network and Dial-Up connection window and select Properties.

**STEP 2:** Enter the TCP/IP screen and change the IP address to the domain of 192.168.1.x/24.



**STEP 3:** Click **OK** to submit the settings.

**STEP 4:** Start your Internet browser with the default IP address 192.168.1.1.

## 3.2 Login Procedure

Perform the following steps to bring up the Web user interface and configure the CT-6382D. To log on to the system from the Web browser, follow the steps below:

**STEP 1:** Start your Internet browser. Type the IP address for the VoIP IAD in the Web address field. For example, if the IP address is 192.168.1.1, type <http://192.168.1.1>

**STEP 2:** You will be prompted to enter your user name and password. Type **root** in the user name and **12345** in the password field, and click **OK**. The password can be changed later in the Web User Interface by selecting the **Management** link.



**STEP 3:** After successfully logging in, you will reach the **Quick Setup** menu.



### 3.3 Default Settings

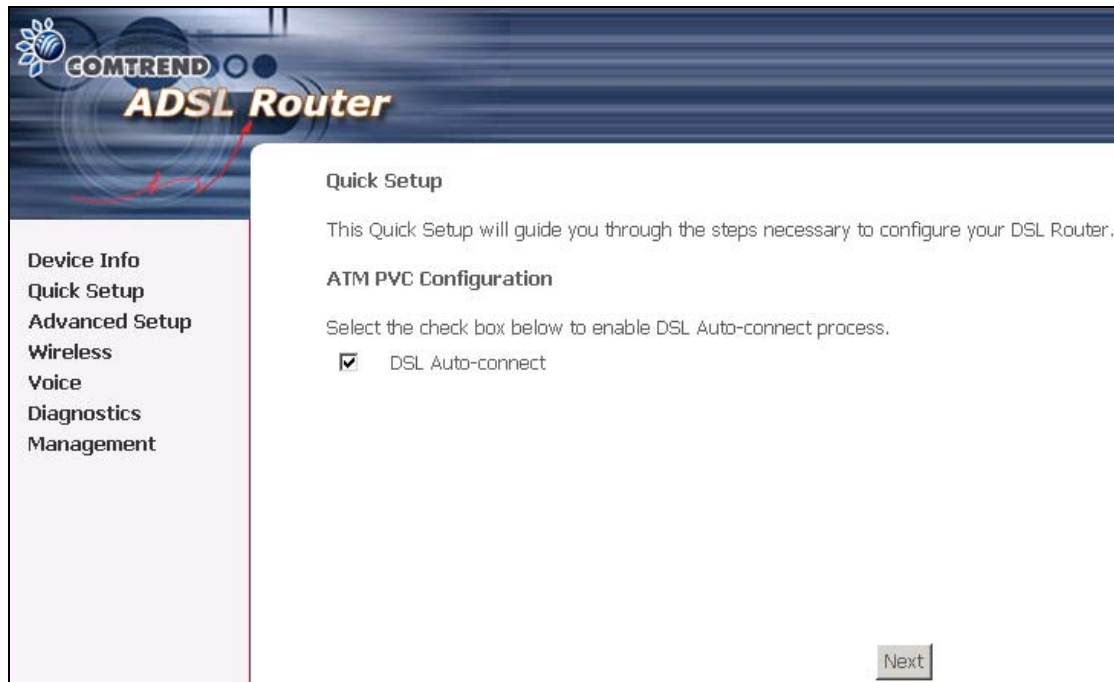
During power on initialization, the CT-6382D initializes all configuration attributes to default values. It will then read the configuration profile from the Permanent Storage section on the flash memory. The default attributes are overridden when identical attributes with different values are configured. The configuration profile in Permanent Storage can be created via the Web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power indicates LED blinking, or by clicking the Restore Default Configuration option in the Restore Settings screen.

The following default settings are present when setting up the VoIP IAD for the first time. The PC running the browser can be attached to the Ethernet.

- LAN port IP address: 192.168.1.1
- Local administrator account name: root
- Local administrator account password: 12345
- Remote WAN access: disabled
- NAT and firewall: enabled
- DHCP server on LAN interface: enabled
- WAN IP address: none

## Chapter 4 Quick Setup


After login, the **Quick Setup** screen appears as shown.



Depending on the network operating mode, and whether NAPT and firewall are enabled or disabled, the main panel will display or hide the NAPT/Firewall menu. For instance, at initial setup, the default network operating mode is Bridge. The main panel will not show the NAPT and Firewall menu.

**Note:** The selections available on the left side of menu are based upon the configured connection.

Shown on the next page for your reference, the **Device Info** screen.



**Device Info**  
Summary  
WAN  
Statistics  
Route  
ARP  
DHCP  
Quick Setup  
Advanced Setup  
Wireless  
Voice  
Diagnostics  
Management

### Device Info

|                           |                      |
|---------------------------|----------------------|
| Board ID:                 | CT6382D-1            |
| Software Version:         | F111-S306CTL_C01_R04 |
| Bootloader (CFE) Version: | 1.0.37-6.5           |
| Wireless Driver Version:  | 3.131.35.0.cpe2.3    |
| ADSL Version:             | A2pB020f.d17m        |

This information reflects the current status of your DSL connection.

|                                |             |
|--------------------------------|-------------|
| Line Rate - Upstream (Kbps):   |             |
| Line Rate - Downstream (Kbps): |             |
| LAN IP Address:                | 192.168.1.1 |
| Default Gateway:               |             |
| Primary DNS Server:            | 192.168.1.1 |
| Secondary DNS Server:          | 192.168.1.1 |

This information reflects the current status of your VoIP connection.

|                           |             |
|---------------------------|-------------|
| Account 1 Current Status: | Direct Mode |
| Account 2 Current Status: | Direct Mode |
| Account 3 Current Status: | Direct Mode |
| Account 4 Current Status: | Direct Mode |

## 4.1 WAN

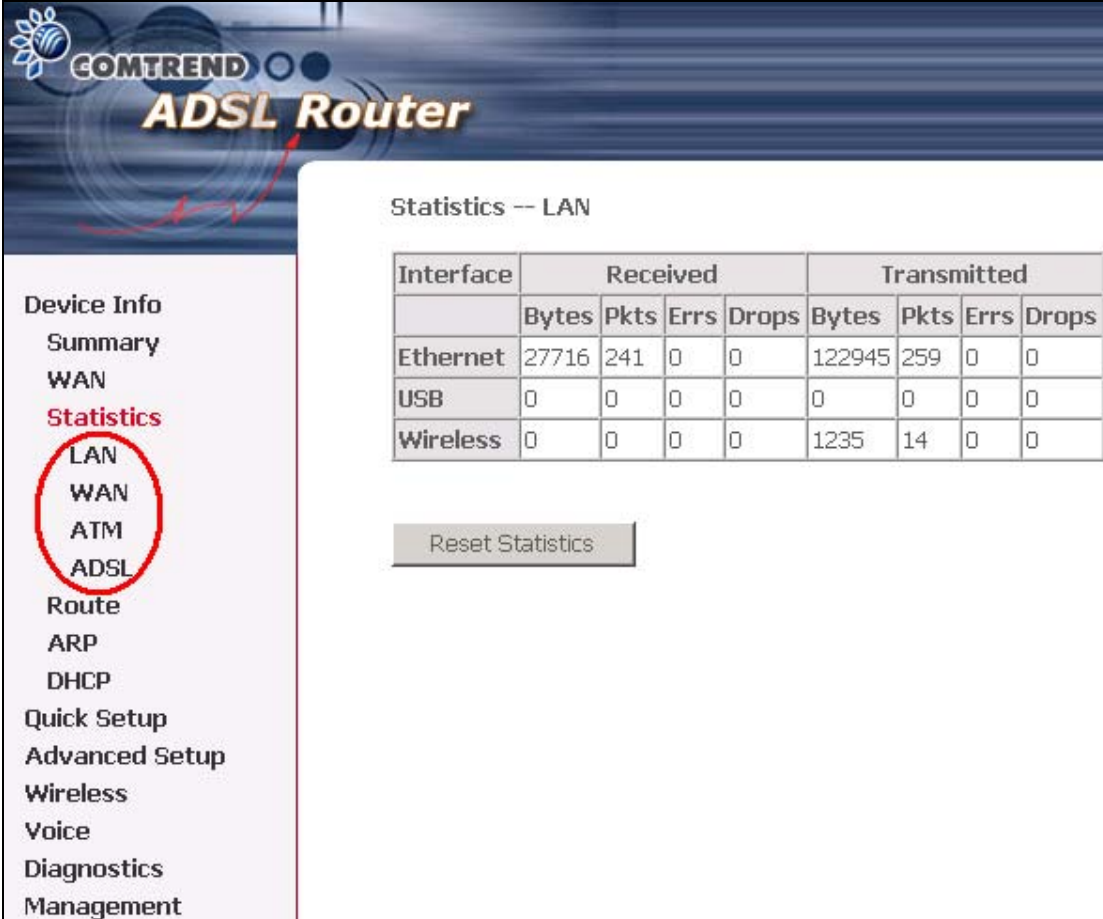
Click **WAN** on the Device Info menu bar to display the configured PVC(s) and the status.



|            |   |
|------------|---|
| VPI/VCI    | Shows the values of the ATM VPI/VCI                   |
| Con. ID    | Shows the connection ID                               |
| Category   | Shows the ATM service classes                         |
| Service    | Shows the name for WAN connection                     |
| Interface  | Shows connection interfaces                           |
| Protocol   | Shows the connection type, such as PPPoE, PPPoA, etc. |
| Igmp       | Shows the status of the IGMP Proxy function           |
| QoS        | Shows if IGMP IP QoS is enabled or disabled           |
| State      | Shows the connection state of the WAN connection      |
| Status     | Lists the status of DSL link                          |
| IP Address | Shows IP address for WAN interface                    |

## 4.2 Statistics

Selection of the Statistics screen provides statistics for the Network Interface of LAN, WAN, ATM and ADSL. All statistics screens are updated every 15 seconds.



COMTREND  
**ADSL Router**

Device Info  
Summary  
WAN  
**Statistics**  
LAN  
WAN  
ATM  
ADSL  
Route  
ARP  
DHCP  
Quick Setup  
Advanced Setup  
Wireless  
Voice  
Diagnostics  
Management

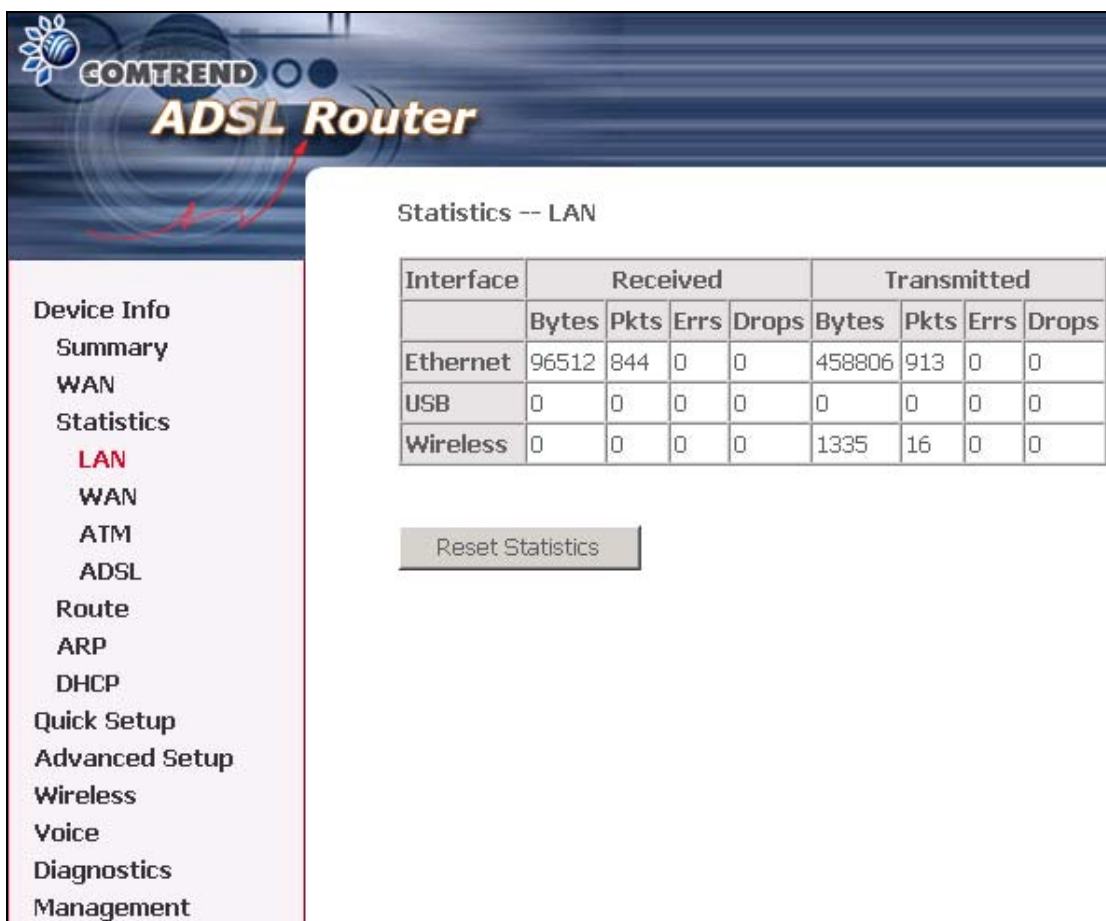
Statistics -- LAN

| Interface | Received |      |      |       | Transmitted |      |      |       |
|-----------|----------|------|------|-------|-------------|------|------|-------|
|           | Bytes    | Pkts | Errs | Drops | Bytes       | Pkts | Errs | Drops |
| Ethernet  | 27716    | 241  | 0    | 0     | 122945      | 259  | 0    | 0     |
| USB       | 0        | 0    | 0    | 0     | 0           | 0    | 0    | 0     |
| Wireless  | 0        | 0    | 0    | 0     | 1235        | 14   | 0    | 0     |

Reset Statistics

### 4.2.1 LAN Statistics

The Network Statistics screen shows interface statistics for ATM AAL5 interface, and Ethernet interfaces. (The Network Statistics screen shows interface statistics for LAN or Ethernet interfaces. This provides byte transfer, packet transfer, Error and Drop statistics for the LAN interface.)

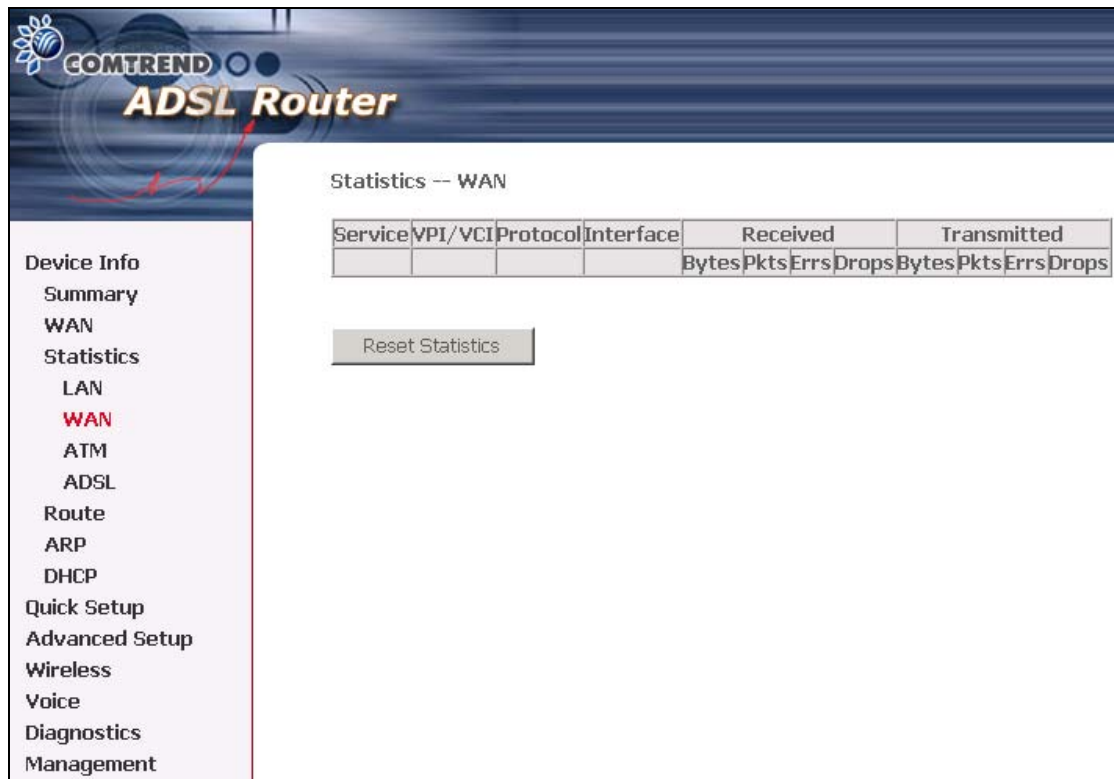


The screenshot displays the Comtrend ADSL Router web interface. The top header features the Comtrend logo and the text "ADSL Router". On the left, a navigation menu lists various settings: Device Info, Summary, WAN, Statistics, LAN (highlighted in red), WAN, ATM, ADSL, Route, ARP, DHCP, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main content area is titled "Statistics -- LAN" and contains a table with interface statistics. Below the table is a "Reset Statistics" button.

| Interface | Received |      |      |       | Transmitted |      |      |       |
|-----------|----------|------|------|-------|-------------|------|------|-------|
|           | Bytes    | Pkts | Errs | Drops | Bytes       | Pkts | Errs | Drops |
| Ethernet  | 96512    | 844  | 0    | 0     | 458806      | 913  | 0    | 0     |
| USB       | 0        | 0    | 0    | 0     | 0           | 0    | 0    | 0     |
| Wireless  | 0        | 0    | 0    | 0     | 1335        | 16   | 0    | 0     |

Reset Statistics

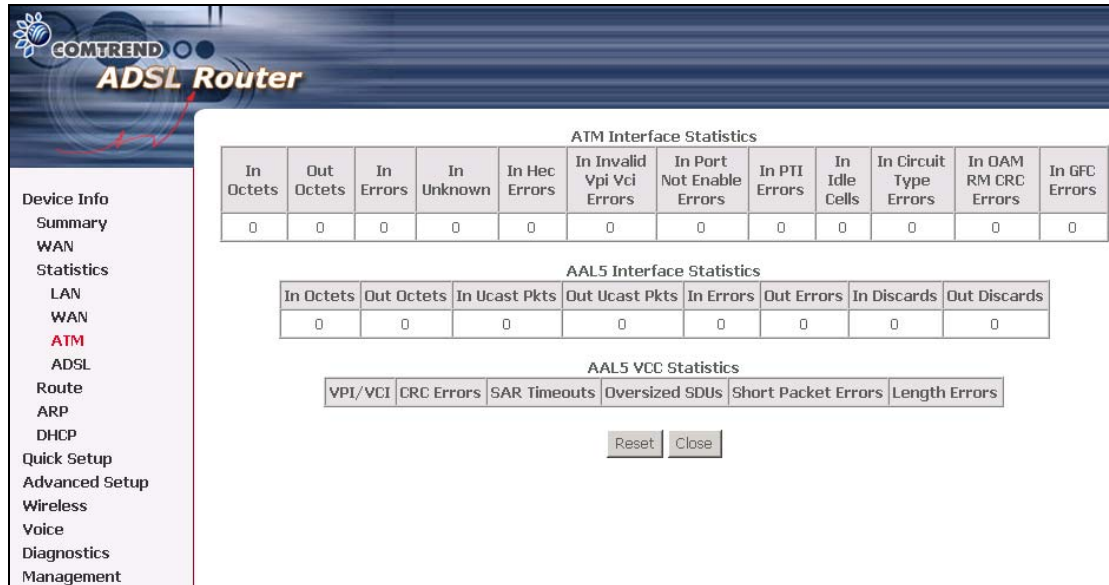
## 4.2.2 WAN Statistics



|                      |   |
|----------------------|---|
| Service              | Shows the service type, as configured by the administrator  |
| VPI/VCI              | Shows the values of the ATM VPI/VCI   |
| Protocol             | Shows the connection type, such as PPPoE, PPPoA, etc.   |
| Interface            | Shows connection interfaces in the following format: nas_(VPI number_VCI number). These interfaces are devised by the system and not the user.  |
| Received/Transmitted | <ul style="list-style-type: none"> <li>- Bytes Rx/TX (receive/transmit) packet in Byte</li> <li>- Pkts Rx/TX (receive/transmit) packets</li> <li>- Errs Rx/TX (receive/transmit) the packets which are errors,</li> <li>- Drops Rx/TX (receive/transmit) the packets which are dropped</li> </ul> |

### 4.2.3 ATM statistics

The following figure shows the ATM statistics screen.



#### ATM Interface Statistics

| Field                      | Description  |
|----------------------------|--|
| In Octets                  | Number of received octets over the interface   |
| Out Octets                 | Number of transmitted octets over the interface  |
| In Errors                  | Number of cells dropped due to uncorrectable HEC errors  |
| In Unknown                 | Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here. |
| In Hec Errors              | Number of cells received with an ATM Cell Header HEX error   |
| In Invalid Vpi Vci Errors  | Number of cells received with an unregistered VCC address.   |
| In Port Not Enabled Errors | Number of cells received on a port that has not been enabled.  |
| In PTI Errors              | Number of cells received with an ATM header Payload Type Indicator (PTI) error   |
| In Idle Cells              | Number of idle cells received  |
| In Circuit Type Errors     | Number of cells received with an illegal circuit type  |
| In OAM RM CRC Errors       | Number of OAM and RM cells received with CRC errors  |
| In GFC Errors              | Number of cells received with a non-zero GFC.  |

### ATM AAL5 Layer Statistics over ADSL interface

| Field          | Description   |
|----------------|---|
| In Octets      | Number of received AAL5/AAL0 CPCS PDU octets  |
| Out Octets     | Number of received AAL5/AAL0 CPCS PDUs octets transmitted   |
| In Ucast Pkts  | Number of received AAL5/AAL0 CPCS PDUs passed to a higher-layer for transmission  |
| Out Ucast Pkts | Number of received AAL5/AAL0 CPCS PDUs received from a higher layer for transmissions                                     |
| In Errors      | Number of received AAL5/AAL0 CPCS PDUs received that contain an error. The types of errors counted include CRC-32 errors. |
| Out Errors     | Number of received AAL5/AAL0 CPCS PDUs that could be transmitted due to errors.   |
| In Discards    | Number of received AAL5/AAL0 CPCS PDUs discarded due to an input buffer overflow condition.                               |
| Out Discards   | This field is not currently used  |

### ATM AAL5 LAYER STATISTICS FOR EACH VCC OVER ADSL INTERFACE

| Field                | Descriptions  |
|----------------------|---|
| CRC Errors           | Number of PDUs received with CRC-32 errors  |
| SAR TimeOuts         | Number of partially re-assembled PDUs which were discarded because they were not fully re-assembled within the required period of time. If the re-assembly time is not supported then, this object contains a zero value. |
| Over Sized SDUs      | Number of PDUs discarded because the corresponding SDU was too large  |
| Short Packets Errors | Number of PDUs discarded because the PDU length was less than the size of the AAL5 trailer  |
| Length Errors        | Number of PDUs discarded because the PDU length did not match the length in the AAL5 trailer  |

#### 4.2.4 ADSL Statistics

The following figure shows the ADSL Network Statistics screen. Within the ADSL Statistics window, a bit Error Rate Test can be started using the ADSL BER Test button. The Reset button resets the statistics.

COMTREND  
**ADSL Router**

Statistics -- ADSL

|                          |            |           |
|--------------------------|------------|-----------|
| Mode:                    |            |           |
| Type:                    |            |           |
| Line Coding:             |            |           |
| Status:                  |            | Link Down |
| Link Power State:        |            | LO        |
|                          |            |           |
|                          | Downstream | Upstream  |
| SNR Margin (dB):         |            |           |
| Attenuation (dB):        |            |           |
| Output Power (dBm):      |            |           |
| Attainable Rate (Kbps):  |            |           |
| Rate (Kbps):             |            |           |
|                          |            |           |
| Super Frames:            |            |           |
| Super Frame Errors:      |            |           |
| RS Words:                |            |           |
| RS Correctable Errors:   |            |           |
| RS Uncorrectable Errors: |            |           |
|                          |            |           |
| HEC Errors:              |            |           |
| OCD Errors:              |            |           |
| LCD Errors:              |            |           |
| Total Cells:             |            |           |
| Data Cells:              |            |           |
| Bit Errors:              |            |           |
|                          |            |           |
| Total ES:                |            |           |
| Total SES:               |            |           |
| Total UAS:               |            |           |

ADSL BER Test      Reset Statistics

| <b>Field</b>            | <b>Description</b>   |
|-------------------------|--|
| Mode                    | Modulation protocol T1.413, G.lite, G.DMT, ADSL2 or ADSL2+                                 |
| Type                    | Channel type Interleave or Fast  |
| Line Coding             | Line Coding format, that can be selected G.dmt, G.lite, T1.413, ADSL2, Annex L and Annex M |
| Status                  | Lists the status of the DSL link   |
| Link Power State        | Link output power state.   |
| SNR Margin (dB)         | Signal to Noise Ratio (SNR) margin   |
| Attenuation (dB)        | Estimate of average loop attenuation in the downstream direction.                          |
| Output Power (dBm)      | Total upstream output power  |
| Attainable Rate (Kbps)  | The sync rate you would obtain.  |
| Rate (Kbps)             | Current sync rate.   |
| Super Frames            | Total number of super frames   |
| Super Frame Errors      | Number of super frames received with errors  |
| RS Words                | Total number of Reed-Solomon code errors   |
| RS Correctable Errors   | Total Number of RS with correctable errors   |
| RS Uncorrectable Errors | Total Number of RS words with uncorrectable errors   |
| HEC Errors              | Total Number of Header Error Checksum errors   |
| OCD Errors              | Total Number of out-of-cell Delineation errors   |
| LCD Errors              | Total number of Loss of Cell Delineation   |
| Total ES:               | Total Number of Errored Seconds  |
| Total SES:              | Total Number of Severely Errored Seconds   |
| Total UAS:              | Total Number of Unavailable Seconds  |

## 4.2.5 Route

Choose **Route** to display the routes that the router has learned.

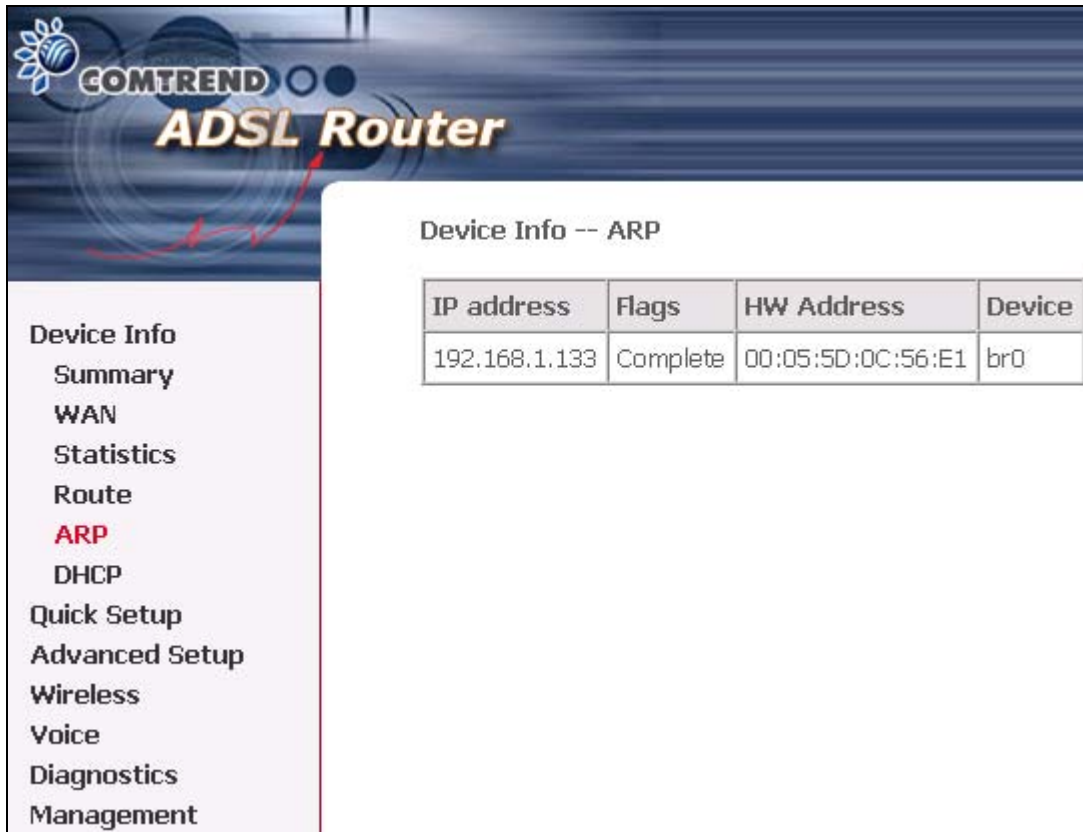
The screenshot shows the Comtrend ADSL Router web interface. On the left is a navigation menu with the following items: Device Info, Summary, WAN, Statistics, **Route** (highlighted in red), ARP, DHCP, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main content area is titled "Device Info -- Route". Below the title, it lists flags: "Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect)." Below the flags is a table with the following data:

| Destination | Gateway | Subnet Mask   | Flag | Metric | Service | Interface |
|-------------|---------|---------------|------|--------|---------|-----------|
| 192.168.1.0 | 0.0.0.0 | 255.255.255.0 | U    | 0      |         | br0       |

| Field       | Description  |
|-------------|--|
| Destination | Destination network or destination host  |
| Gateway     | Next hop IP address  |
| Subnet Mask | Subnet Mask of Destination   |
| Flag        | U: route is <b>up</b><br>!: <b>reject</b> route<br>G: use <b>gateway</b><br>H: target is a <b>host</b><br>R: <b>reinstate</b> route for dynamic routing<br>D: <b>dynamically</b> installed by daemon or redirect<br>M: <b>modified</b> from routing daemon or redirect |
| Metric      | The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.  |
| Service     | Shows the name for WAN connection  |
| Interface   | Shows connection interfaces  |

## 4.2.6 ARP

Click **ARP** to display the ARP information.

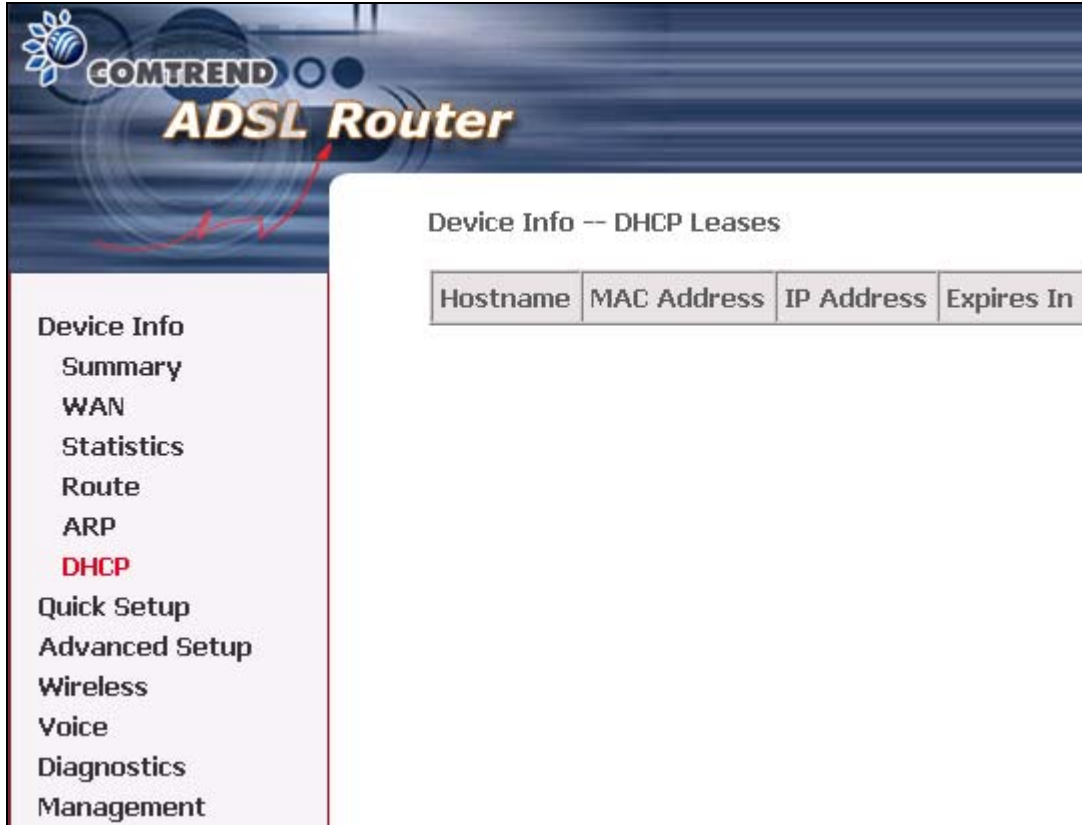


The screenshot displays the Comtrend ADSL Router web interface. The header features the Comtrend logo and the text "ADSL Router". A left-hand navigation menu lists various settings: Device Info, Summary, WAN, Statistics, Route, **ARP** (highlighted in red), DHCP, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main content area is titled "Device Info -- ARP" and contains a table with the following data:

| IP address    | Flags    | HW Address        | Device |
|---------------|----------|-------------------|--------|
| 192.168.1.133 | Complete | 00:05:5D:0C:56:E1 | br0    |

#### 4.2.7 DHCP

Click **DHCP** to display the DHCP Leases information.



The screenshot displays the Comtrend ADSL Router web interface. The top banner features the Comtrend logo and the text "ADSL Router". On the left, a vertical navigation menu lists various settings: Device Info, Summary, WAN, Statistics, Route, ARP, **DHCP** (highlighted in red), Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main content area is titled "Device Info -- DHCP Leases" and contains a table with the following headers: Hostname, MAC Address, IP Address, and Expires In. The table body is currently empty.

| Hostname | MAC Address | IP Address | Expires In |
|----------|-------------|------------|------------|
|----------|-------------|------------|------------|

## Chapter 5 Quick Setup

The Quick Setup option will not be displayed in the menu bar if a WAN is configured. The Quick Setup allows the user to configure the ADSL VoIP IAD for DSL connectivity and Internet access. It also guides the user through the WAN network setup first and then the LAN interface setup. You can either manually customize the VoIP IAD or follow the online instruction to set up the VoIP IAD.

The CT-6382D ADSL VoIP IAD supports the following five network operating modes over an ATM PVC WAN interface.

- PPP over Ethernet (PPPoE)
- PPP over ATM (PPPoA)
- MAC Encapsulated Routing (MER)
- IP over ATM (IPoA)
- Bridging (default)

The following configuration considerations apply:

- The WAN network operating mode operation depends on the service provider's configuration on the Central Office side and Broadband Access Server for the PVC
- If the service provider provides PPPoE service, then the connection selection depends on whether the LAN-side device (typically a PC) is running a PPPoE client or whether the CT-6382D is to run the PPPoE client. The CT-6382D can support both cases simultaneously.
- If some or none of the LAN-side devices do not run PPPoE client, then select PPPoE. If every LAN-side device is running a PPPoE client, then select Bridge. In PPPoE mode, CT-6382D also supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client and non-PPPoE LAN devices.
- NAPT and firewall are always enabled when PPPoE mode is selected, but they can be enabled or disabled by the user when MER or IPoA is selected, NAPT and firewall are always disabled when Bridge mode is selected.

**Note:** Up to eight PVC profiles can be configured and saved on the flash memory. To activate a particular PVC profile, you need to navigate all the Quick Setup pages until the last summary page, then click on the Finish button and reboot the system.

## 5.1 Auto Quick Setup

The auto quick setup requires the ADSL link to be up. The ADSL VoIP IAD will automatically detect the PVC. You only need to follow the online instructions that you are prompted.

1. Select **Quick Setup** to display the DSL Quick Setup screen.



2. Click **Next** to start the setup process. Follow the online instructions to complete the setting. This procedure will skip some processes like PVC index, or encapsulation.
3. After the settings are complete, you can use the ADSL service.

## 5.2 Manual Quick Setup

**STEP 1:** Click **Quick Setup** and un-tick the **DSL Auto-connect** checkbox to enable manual configuration of the connection type.



**COMTREND ADSL Router**

**Quick Setup**

This Quick Setup will guide you through the steps necessary to configure your DSL Router.

**ATM PVC Configuration**

Select the check box below to enable DSL Auto-connect process.

☒ DSL Auto-connect

**Device Info**  
**Quick Setup**  
Advanced Setup  
Wireless  
Voice  
Diagnostics  
Management

Un-tick this checkbox to enable manual setup and display the following screen.

The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.

VPI: [0-255]

VCI: [32-65535]

**Enable Quality Of Service**

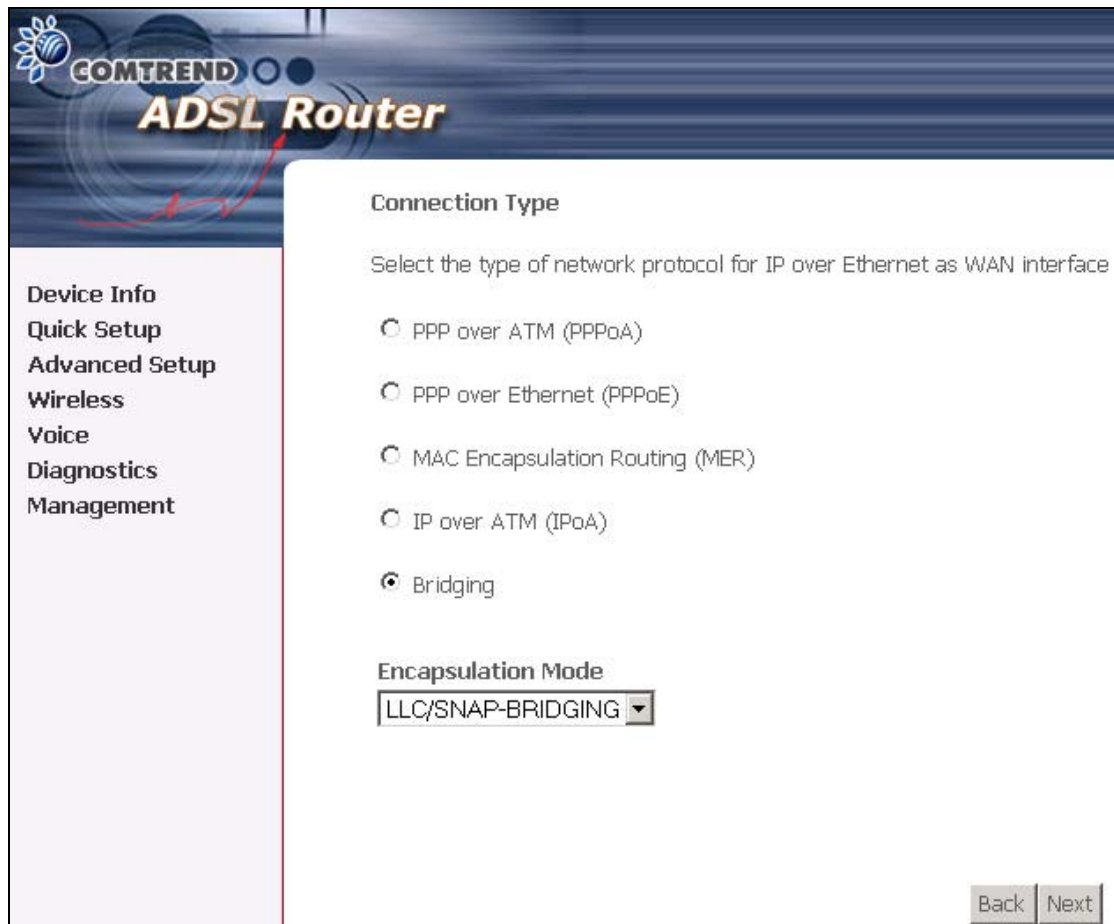
Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service ☐

**Next**

**STEP 2:** Enter the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). Select Enable Quality of Service if required. Click **Next**.

**STEP 3:** Then, choose the Encapsulation mode.



The screenshot displays the configuration interface for a COMTREND ADSL Router. On the left is a vertical navigation menu with the following items: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main content area is titled "Connection Type" and includes the instruction: "Select the type of network protocol for IP over Ethernet as WAN interface". Below this instruction are five radio button options: "PPP over ATM (PPPoA)", "PPP over Ethernet (PPPoE)", "MAC Encapsulation Routing (MER)", "IP over ATM (IPoA)", and "Bridging". The "Bridging" option is selected, indicated by a filled radio button. Below the radio buttons is a section titled "Encapsulation Mode" with a dropdown menu currently showing "LLC/SNAP-BRIDGING". At the bottom right of the configuration area are two buttons: "Back" and "Next".

**STEP 4:** Click **Next** to display the following screen. Choosing different connection types pops up different settings requests. Enter appropriate settings that are requested by your service provider. The following descriptions state each connection type setup separately.

## 5.2.1 PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE)

1. Select the **PPP over ATM (PPPoA)** or **PPP over Ethernet (PPPoE)** radio button and click **Next**. The following screen appears:

The screenshot shows the 'PPP Username and Password' configuration page of a COMTREND ADSL Router. The page has a blue header with the COMTREND logo and 'ADSL Router' text. On the left, there is a navigation menu with links: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main content area is titled 'PPP Username and Password' and includes a descriptive paragraph: 'PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.' Below this, there are four input fields: 'PPP Username:', 'PPP Password:', 'PPPoE Service Name:', and 'Authentication Method:' (which is a dropdown menu currently set to 'AUTO'). There are also five checkboxes: 'Dial on demand (with idle timeout timer)', 'PPP IP extension', 'Use Static IP Address', and 'Enable PPP Debug Mode'. At the bottom right, there are 'Back' and 'Next' buttons.

### PPP Username/PPP Password

The PPP Username and the PPP password requirement are dependent on the particular requirements of the ISP or the ADSL service provider. The WEB user interface allows a maximum of 256 characters in the PPP user name and a maximum of 32 characters in PPP password.

### PPPoE service name

For PPPoE service, PADI requests contain a service name-tag. Some PPPoE servers (or BRAS) of ISP check this service name-tag for connection.

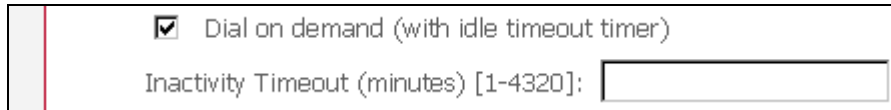
### Encapsulation Mode

Choosing different connection types provides different encapsulation modes.

- PPPoA- VC/MUX, LLC/ENCAPSULATION
- PPPoE- LLC/SNAP BRIDGING, VC/MUX
- MER- LLC/SNAP-BRIDGING, VC/MUX
- IPoA- LLC/SNAP-ROUTING, VC/MUX
- Bridging- LLC/SNAP-BRIDGING, VC/MUX

### Disconnect if no activity

The CT-6382D can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** check box. When the checkbox is ticked, you need to enter the inactivity timeout period. The timeout period ranges from 1 minute to 4320 minutes.



☒ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

### PPP IP Extension

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specially requires this setup, do not select it.

The PPP IP Extension supports the following conditions:

- Allows only one PC on the LAN
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC's LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the ADSL VoIP IAD has a single IP address to assign to a LAN device.
- NAPT and firewall are disabled when this option is selected.
- The ADSL VoIP IAD becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The ADSL VoIP IAD extends the IP subnet at the remote service provider to the LAN PC. That is, the PC becomes a host belonging to the same IP subnet.
- The ADSL VoIP IAD bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the VoIP IAD's LAN IP address.

### Use Static IP Address

Unless your service provider specially requires this setup, do not select it.

If selected, enter your static IP address.

### Enable PPP Debug Mode

Enable the PPPoE debug mode. The system will put more PPP connection information in System Log. But this is for debug, please don't enable in normal usage.

2. Click **Next** to display the following screen.

COMTREND  
**ADSL Router**

Device Info  
Quick Setup  
Advanced Setup  
Wireless  
Voice  
Diagnostics  
Management

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast ☐

Enable WAN Service ☒

Service Name

Back Next

**Enable IGMP Multicast checkbox:** Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast IAD's.

**Enable WAN Service checkbox:** Tick this item to enable the ADSL service. Untick it to stop the ADSL service.

**Service Name:** This is user-defined.

3. After entering your settings, select **Next**.

The Device Setup page allows the user to configure the LAN interface IP address and DHCP server. If the user would like this ADSL router to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP server on the LAN** to enter the starting IP address and end IP address and DHCP lease time. This configures the router to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Note that the router's default IP address is 192.168.1.1 and the default private address range provided by the ISP server in the router is 192.168.1.2 through 192.168.1.254.

COMTREND  
ADSL Router

Device Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

Leased Time (hour): 24

☐ Configure the second IP Address and Subnet Mask for LAN interface

Back Next

To configure a secondary IP address for the LAN port, click the box as shown here.

☒ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

4. Click Next and the screen below will be displayed.

5. To enable the wireless function, select the box (by clicking on it) and input the SSID. Then, click **Next**.

**Wireless -- Setup**

Enable Wireless ☒

Enter the wireless network name (also known as SSID):

SSID:

Back Next

6. Click **Next** to display the WAN Setup-Summary screen that presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.

|                     |                        |
|---------------------|------------------------|
| VPI / VCI:          | 0 / 35                 |
| Connection Type:    | PPPoE                  |
| Service Name:       | pppoe_0_35_1           |
| Service Category:   | UBR                    |
| IP Address:         | Automatically Assigned |
| Service State:      | Enabled                |
| NAT:                | Enabled                |
| Firewall:           | Enabled                |
| IGMP Multicast:     | Disabled               |
| Quality Of Service: | Disabled               |

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications  
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

Back Save/Reboot

7. After clicking **Save/Reboot**, the VoIP IAD will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-6382D is ready for operation and the LEDs display as described in the LED description tables.

## 5.2.2 MAC Encapsulation Routing (MER)

To configure MER, do the following.

1. Select **Quick Setup** and click **Next**.
2. Enter the PVC Index provided by the ISP and click **Next**.
3. Select the MAC Encapsulation Routing (MER) radio button, and click **Next**. The following screen appears.

The screenshot shows the WAN IP Settings page of a COMTREND ADSL Router. The page has a blue header with the COMTREND logo and 'ADSL Router' text. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main content area is titled 'WAN IP Settings' and contains a notice about DHCP and static configurations. It features three radio button options for IP address assignment: 'Obtain an IP address automatically' (selected), 'Use the following IP address:', and 'Obtain default gateway automatically' (selected). Below these are input fields for WAN IP Address, WAN Subnet Mask, and default gateway (with sub-options for IP Address and WAN Interface). At the bottom are fields for Primary and Secondary DNS server addresses, and 'Back' and 'Next' buttons.

**COMTREND ADSL Router**

**WAN IP Settings**

Enter information provided to you by your ISP to configure the WAN IP settings.  
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.  
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

☒ Obtain an IP address automatically  
☐ Use the following IP address:  
WAN IP Address:   
WAN Subnet Mask:

☒ Obtain default gateway automatically  
☐ Use the following default gateway:  
☐ Use IP Address:   
☒ Use WAN Interface: mer\_0\_35/nas\_0\_35

☒ Obtain DNS server addresses automatically  
☐ Use the following DNS server addresses:  
Primary DNS server:   
Secondary DNS server:

Back Next

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: DHCP can be enabled for PVC in MER mode if **Obtain an IP address automatically** is chosen. Changing the default gateway or the DNS affects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.

If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

The ISP should provide the values that must be entered in the entry fields.

4. Click **Next** to display the following screen appears.

The screenshot shows the 'Network Address Translation Settings' page of a COMTREND ADSL Router. The left sidebar contains a menu with the following items: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main content area is titled 'Network Address Translation Settings' and includes a descriptive paragraph: 'Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).' Below this, there are three checkboxes: 'Enable NAT' (checked), 'Enable Firewall' (checked), and 'Enable IGMP Multicast, and WAN Service'. Under the third checkbox, there are two sub-options: 'Enable IGMP Multicast' (unchecked) and 'Enable WAN Service' (checked). A 'Service Name' field contains the text 'mer\_0\_35'. At the bottom right, there are 'Back' and 'Next' buttons.

**Enable NAT checkbox:** If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel.

**Enable Firewall checkbox:** If the firewall checkbox is selected, the firewall submenu on the left side main panel will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Firewall submenu will not be displayed on the left main panel.

**Enable IGMP Multicast:** Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast VoIP IAD's.

**Enable WAN Service:** Tick the checkbox to enable the WAN (ADSL) service. If this item is not selected, you will not be able to use the ADSL service.

**Service Name:** This is User-defined.

5. Upon completion, click **Next**. The following screen appears.

**COMTREND ADSL Router**

**Device Setup**

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address:

Subnet Mask:

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

☐ Configure the second IP Address and Subnet Mask for LAN interface

The Device Setup page allows the user to configure the LAN interface IP address and DHCP server. If the user would like this VoIP IAD to assign dynamic IP addresses, DNS server and default gateway to other LAN devices, select the radio box **Enable DHCP server** to enter the starting IP address and end IP address and DHCP lease time. This configures the IAD to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Note that the IAD's default IP address is 192.168.1.1 and the default private address range provided by the DHCP server in the IAD is 192.168.1.2 through 192.168.1.254.

**Note:** The Ethernet interface (and the wireless LAN interface on the CT-6382D) share the same subnet since they are bridged within the IAD.

6. After entering your settings, select **Next** to display the following screen. The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

7. The following screen will be displayed. To enable the wireless function, select the box (by clicking on it) and input the SSID. Then, click **Next**.

### Wireless -- Setup

Enable Wireless ☒

Enter the wireless network name (also known as SSID).

SSID:

Back Next

The following screen will be displayed.

## COMTREND ADSL Router

Device Info

Quick Setup

Advanced Setup

Wireless

Voice

Diagnostics

Management

### WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

|                     |                        |
|---------------------|------------------------|
| VPI / VCI:          | 0 / 35                 |
| Connection Type:    | MER                    |
| Service Name:       | mer_0_35               |
| Service Category:   | UBR                    |
| IP Address:         | Automatically Assigned |
| Service State:      | Enabled                |
| NAT:                | Enabled                |
| Firewall:           | Enabled                |
| IGMP Multicast:     | Disabled               |
| Quality Of Service: | Disabled               |

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.  
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

Back Save/Reboot

After clicking **Save/Reboot**, the IAD will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-6382D is ready for operation and the LEDs display as described in the LED description tables.

### 5.2.3 IP Over ATM

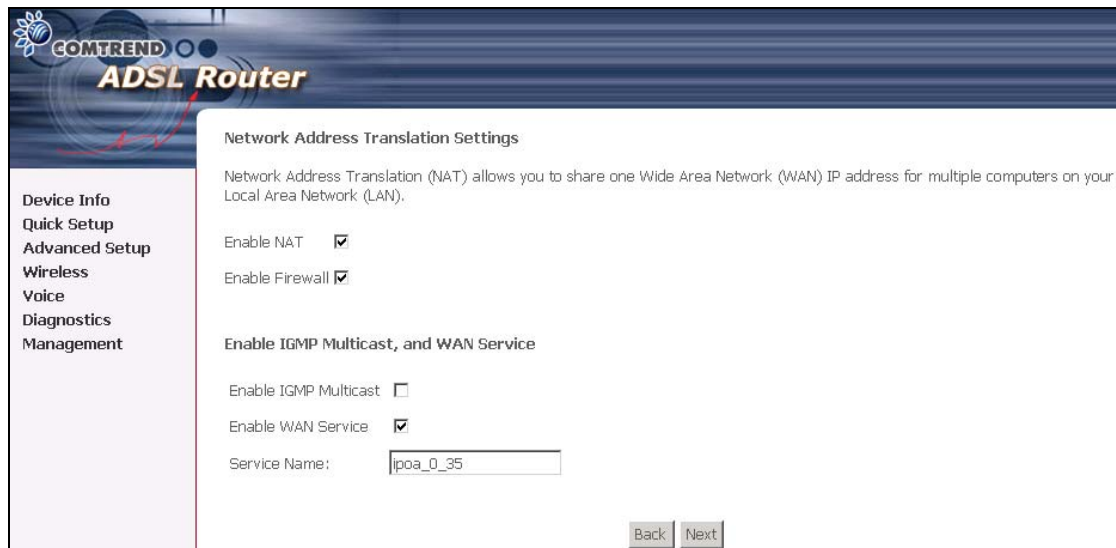
To configure IP Over ATM,

1. Select **Quick Setup** and click **Next**.
2. Enter the PVC Index and click **Next**.
3. Type the VPI and VCI values provided by the ISP and click **Next**.
4. Select the IP over ATM (IPoA) radio button and click **Next**. The following screen appears.

The screenshot shows the WAN IP Settings page of a COMTREND ADSL Router. The page has a blue header with the COMTREND logo and 'ADSL Router' text. On the left is a navigation menu with links: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main content area is titled 'WAN IP Settings' and contains the following text: 'Enter information provided to you by your ISP to configure the WAN IP settings.' and a notice: 'Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection.' Below this are input fields for 'WAN IP Address' (0.0.0.0) and 'WAN Subnet Mask' (0.0.0.0). There are two main sections for configuration, each with a checkbox. The first section is 'Use the following default gateway:' with sub-options 'Use IP Address:' (checkbox) and 'Use WAN Interface:' (checkbox, with a dropdown menu showing 'ipoa\_0\_35/ipa\_0\_35'). The second section is 'Use the following DNS server addresses:' with sub-options 'Primary DNS server:' and 'Secondary DNS server:' (both with input fields). At the bottom right are 'Back' and 'Next' buttons.

Notice that **Obtain an IP address automatically** (DHCP client) is not supported over IPoA. The user must enter the IP address or WAN interface for the default gateway setup, and the DNS server addresses provided by the ISP.

5. Click **Next**. The following screen appears.



### Enable NAT checkbox

If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be de-selected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel.

### Enable Firewall checkbox

If the firewall checkbox is selected, the firewall submenu on the left side main panel will be displayed after system reboot. The user can then configure firewall features after the system comes up. If firewall is not used, this checkbox should be de-selected to free up system resources for better performance. When system comes back after reboot, the Firewall submenu will not be displayed on the left main panel.

6. Click **Next** to display the following screen. The Device Setup page allows the user to configure the LAN interface IP address and DHCP server if the user would like this VoIP IAD to assign dynamic IP addresses, DNS server and default gateway to other LAN devices. Select the button Enable DHCP server on the LAN to enter the starting IP address and end IP address and DHCP lease time.

**COMTREND**  
**ADSL Router**

**Device Info**  
**Quick Setup**  
**Advanced Setup**  
**Wireless**  
**Voice**  
**Diagnostics**  
**Management**

**Device Setup**

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address:

Subnet Mask:

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

☐ Configure the second IP Address and Subnet Mask for LAN interface

The user must configure the IP Address and the Subnet Mask. To use the DHCP service on the LAN, select the **Enable DHCP server** checkbox, and enter the Start IP addresses, the End IP address and DHCP lease time. This configures the IAD to automatically assign IP addresses, default gateway address and DNS server addresses to each of your PCs.

Note that the IAD's default IP address is 192.168.1.1 and the default private address range provided by DHCP server in the IAD is 192.168.1.2 through 192.168.1.254.

7. The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

8. The following screen will be displayed. To enable the wireless function, select the box (by clicking on it) and input the SSID. Then, click **Next**.

**Wireless -- Setup**

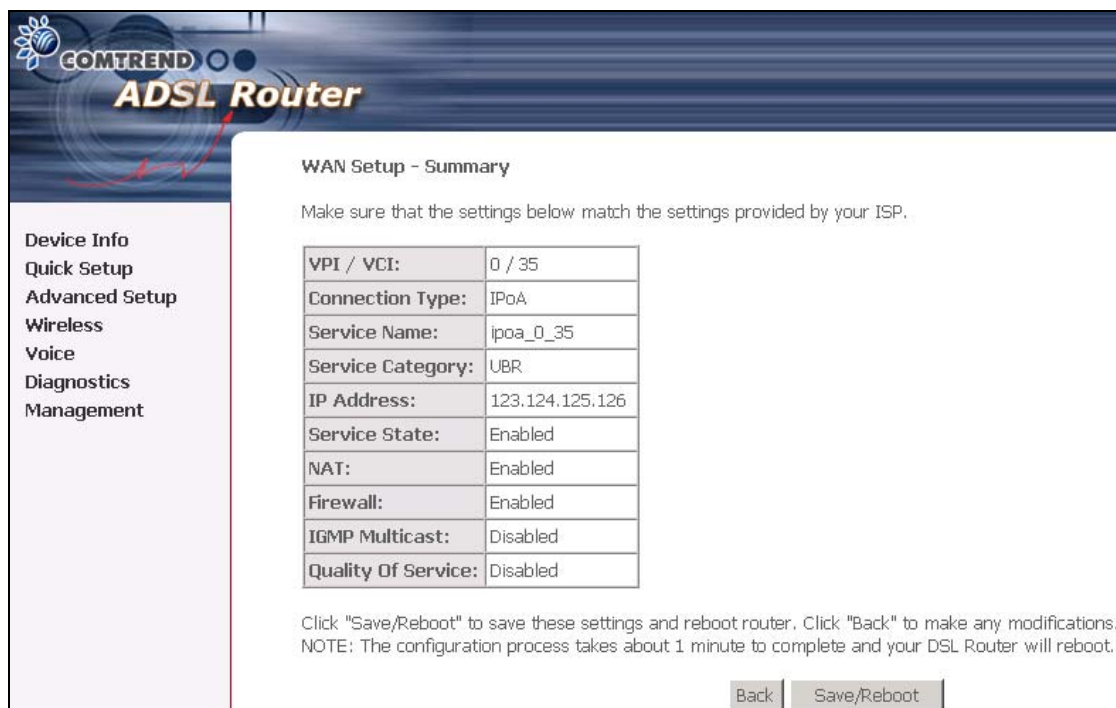
Enable Wireless ☒

Enter the wireless network name (also known as SSID).

SSID:

[Back](#) [Next](#)

The following screen will be displayed.



**COMTREND ADSL Router**

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.

|                     |                 |
|---------------------|-----------------|
| VPI / VCI:          | 0 / 35          |
| Connection Type:    | IPoA            |
| Service Name:       | ipoa_0_35       |
| Service Category:   | UBR             |
| IP Address:         | 123.124.125.126 |
| Service State:      | Enabled         |
| NAT:                | Enabled         |
| Firewall:           | Enabled         |
| IGMP Multicast:     | Disabled        |
| Quality Of Service: | Disabled        |

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.  
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

[Back](#) [Save/Reboot](#)

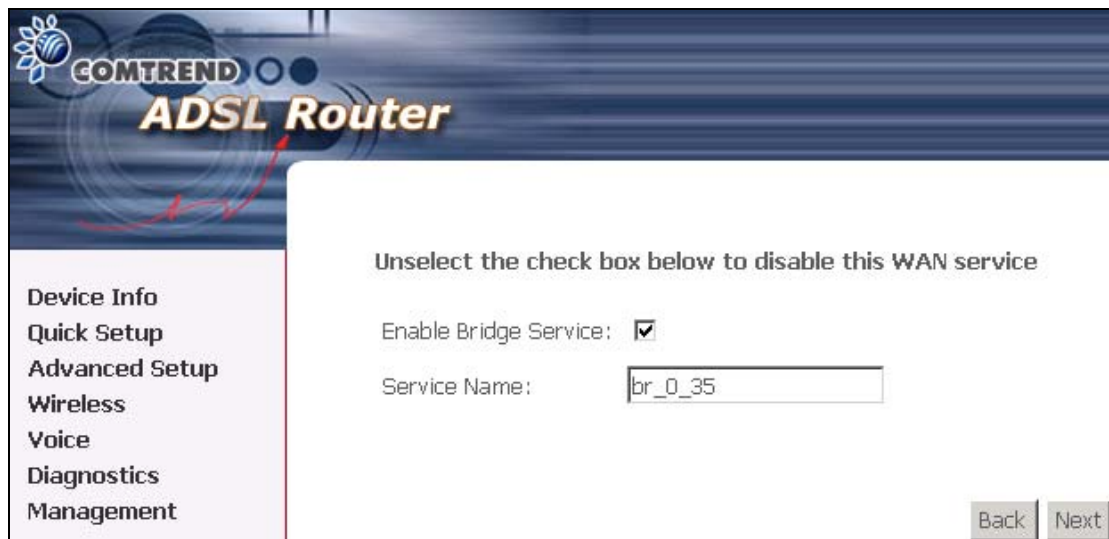
**Device Info**  
Quick Setup  
Advanced Setup  
Wireless  
Voice  
Diagnostics  
Management

9. After clicking **Save/Reboot**, the IAD will save the configuration to the flash memory, and reboot. The Web UI will not respond until the system is brought up again. After the system is up, the Web UI will refresh to the Device Info page automatically. The CT-6382D is ready for operation and the LEDs display as described in the LED description tables.

## 5.2.4 Bridging

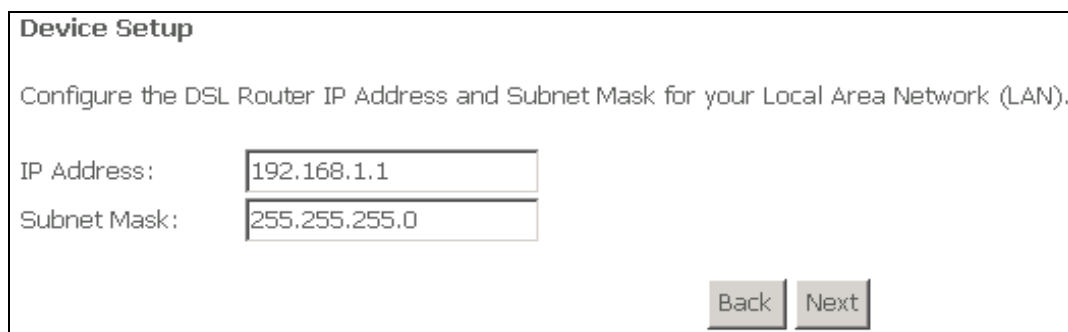
Select the bridging mode. To configure Bridging, do the following.

1. Select Quick Setup and click **Next**.
2. Enter the PVC Index and click **Next**.
3. Type in the VPI and VCI values provided by the ISP and click Next.
4. Select the Bridging radio button and click **Next**. The following screen appears.  
To use the bridge service, tick the checkbox, Enable Bridge Service, and enter the service name.



The screenshot shows the COMTREND ADSL Router configuration interface. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, and Management. The main area has a header with the COMTREND logo and 'ADSL Router'. Below the header, it says 'Unselect the check box below to disable this WAN service'. There is a checkbox labeled 'Enable Bridge Service:' which is checked. Below that is a text field labeled 'Service Name:' containing the text 'br\_0\_35'. At the bottom right are 'Back' and 'Next' buttons.

5. Click the **Next** button to continue. Enter the IP address for the LAN interface. The default IP address is 192.168.1.1. The LAN IP interface in bridge operating mode is needed for local users to manage the VoIP IAD. Notice that there is no IP address for the WAN interface in bridge mode, and the remote technical support cannot access the VoIP IAD. DHCP server is disabled on the LAN.



The screenshot shows the 'Device Setup' screen. It has a title 'Device Setup' and a subtitle 'Configure the DSL Router IP Address and Subnet Mask for your Local Area Network (LAN)'. There are two text input fields: 'IP Address:' with the value '192.168.1.1' and 'Subnet Mask:' with the value '255.255.255.0'. At the bottom right are 'Back' and 'Next' buttons.

6. The following screen will be displayed. To enable the wireless function, select the box (by clicking on it) and input the SSID. Then, click **Next**.


**Wireless -- Setup**

Enable Wireless ☒

Enter the wireless network name (also known as SSID).

SSID:

The following screen will be displayed.



**Device Info**  
**Quick Setup**  
**Advanced Setup**  
**Wireless**  
**Voice**  
**Diagnostics**  
**Management**

**WAN Setup - Summary**  
Make sure that the settings below match the settings provided by your ISP.

|                     |                |
|---------------------|----------------|
| VPI / VCI:          | 0 / 35         |
| Connection Type:    | Bridge         |
| Service Name:       | br_0_35        |
| Service Category:   | UBR            |
| IP Address:         | Not Applicable |
| Service State:      | Enabled        |
| NAT:                | Enabled        |
| Firewall:           | Enabled        |
| IGMP Multicast:     | Not Applicable |
| Quality Of Service: | Disabled       |

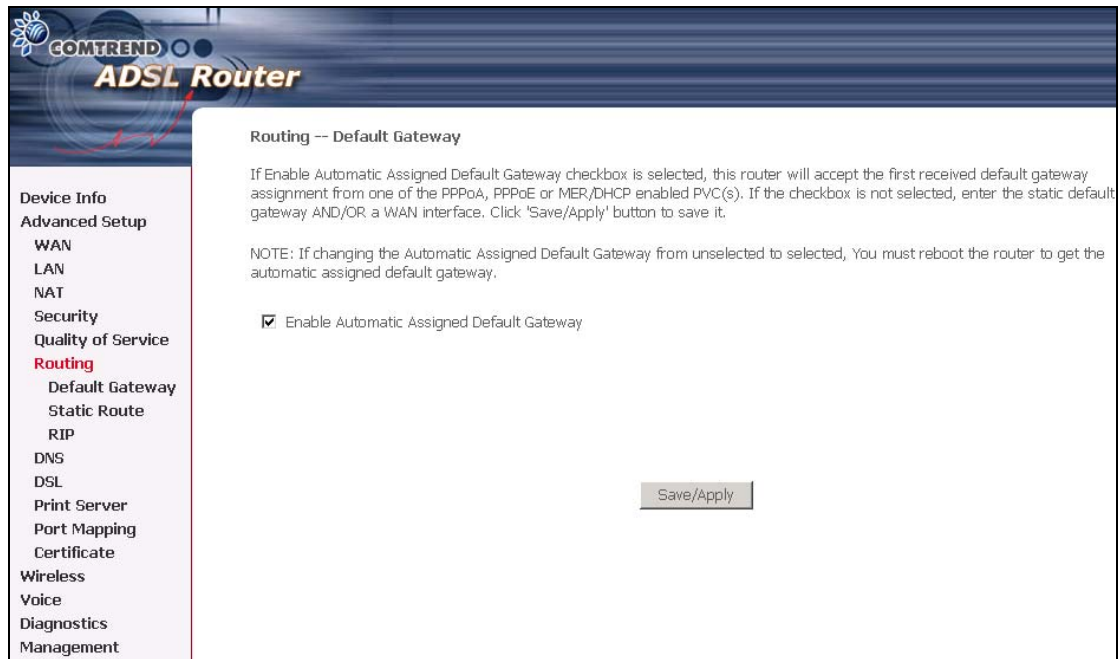
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.  
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

7. The WAN Setup-Summary screen presents the entire configuration summary. Click **Save/Reboot** if the settings are correct. Click **Back** if you wish to modify the settings.

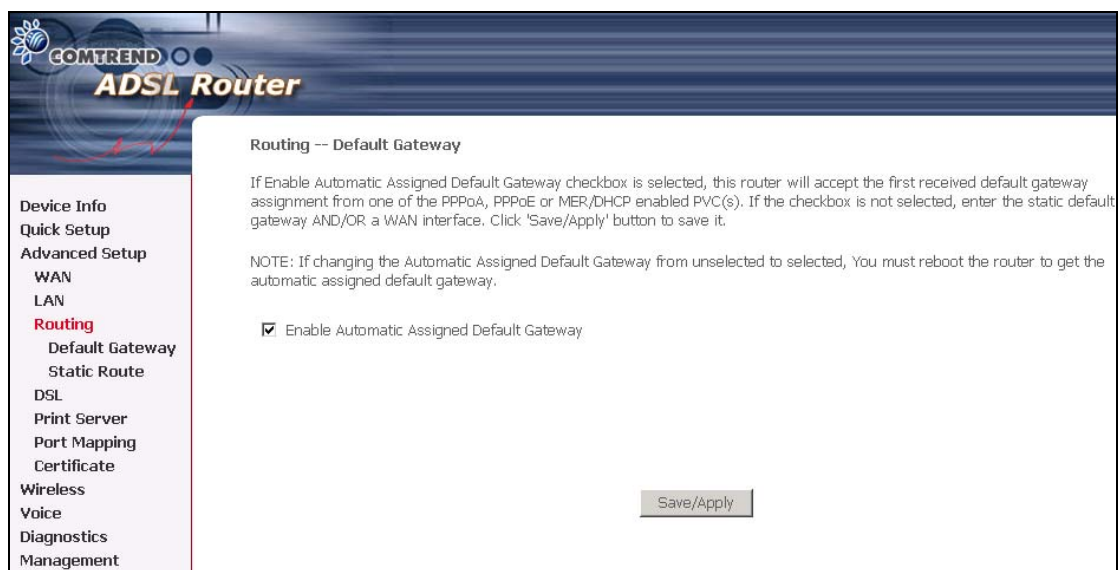
## Chapter 6 Advanced Setup

This chapter explains: WAN, LAN, Routing, DSL and Port Mapping.....

**Note:** Shown below for your reference are the available menu options for each different configuration.



This screenshot is for Mer and IPoA encapsulations.



This screenshot is for PPPoE and PPPoA encapsulations.

COMTREND

ADSL Router

Device Info

Advanced Setup

WAN

LAN

Security

MAC Filtering

Parental Control

Quality of Service

Routing

DSL

Print Server

Port Mapping

Certificate

Wireless

Voice

Diagnostics

Management

MAC Filtering Setup

MAC Filtering Global Policy: **FORWARDED**

Change Policy

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Choose Add or Remove to configure MAC filtering rules.

| VPI/VCI              | Protocol | Destination MAC | Source MAC | Frame Direction | Remove |
|----------------------|----------|-----------------|------------|-----------------|--------|
| <div>AddRemove</div> |          |                 |            |                 |        |

This screenshot is for Bridged encapsulation.

## 6.1 WAN

COMTREND ADSL Router

Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.  
Choose Save/Reboot to apply the changes and reboot the system.

| VPI/VCI | Con. ID | Category | Service | Interface | Protocol | Igmp | QoS | VlanId | State | Remove | Edit |
|---------|---------|----------|---------|-----------|----------|------|-----|--------|-------|--------|------|
|---------|---------|----------|---------|-----------|----------|------|-----|--------|-------|--------|------|

Add Remove Save/Reboot

|           |   |
|-----------|---|
| VPI/VCI   | ATM VPI (0-255) / VCI (32-65535)  |
| Con. ID   | ID for WAN connection   |
| Category  | ATM service category, e.g. UBR, CBR...  |
| Service   | Name of the WAN connection  |
| Interface | Name of the interface for WAN   |
| Protocol  | Shows bridge or router mode   |
| Igmp      | Shows enable or disable IGMP proxy  |
| QoS       | Shows enable or disable IGMP QoS  |
| State     | Shows enable or disable WAN connection  |
| VlanId    | VLAN ID is the identification of the VLAN, which is basically used by the IEEE - 802.1Q |

For further information on WAN please reference section: 4.1, Page 24.

## 6.2 LAN

Configure the VoIP IAD IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the IAD to make the new configuration effective.

**IP Address:** Enter the IP address for the LAN port.

**Subnet Mask:** Enter the subnet mask for the LAN port.

COMTREND ADSL Router

Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address:

Subnet Mask:

☐ Enable IGMP Snooping

☒ Standard Mode

☐ Blocking Mode

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

☐ Enable DHCP Server Relay

DHCP Server IP Address:

☐ Configure the second IP Address and Subnet Mask for LAN interface

Save Save/Reboot

To configure a secondary IP address for the LAN port, click the box as shown below.

☒ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

Save Save/Reboot

**IP Address:** Enter the secondary IP address for the LAN port.

**Subnet Mask:** Enter the secondary subnet mask for the LAN port.

## 6.3 NAT

**Note:** This option is not available for bridge mode.

To display the NAT function, you need to enable the NAT feature in the WAN Setup.

### 6.3.1 Virtual Servers

**Note:** This option is not available for Bridge mode.

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

COMTREND  
**ADSL Router**

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

| Server Name | External Port Start | External Port End | Protocol | Internal Port Start | Internal Port End | Server IP Address | Remove |
|-------------|---------------------|-------------------|----------|---------------------|-------------------|-------------------|--------|
|-------------|---------------------|-------------------|----------|---------------------|-------------------|-------------------|--------|

To add a Virtual Server, simply click the Add button. The following will be displayed.

**COMTREND ADSL Router**

**NAT -- Virtual Servers**

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**  
 Remaining number of entries that can be configured:32

Server Name:  
☒ Select a Service: Select One  
☐ Custom Server:

Server IP Address:

| External Port Start  | External Port End    | Protocol | Internal Port Start  | Internal Port End    |
|----------------------|----------------------|----------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | TCP      | <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> | TCP      | <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> | TCP      | <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> | TCP      | <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> | TCP      | <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> | TCP      | <input type="text"/> | <input type="text"/> |

|   |   |
|---|---|
| Select a Service<br>Or<br>Custom Server | User should select the service from the list.<br>Or<br>User can enter the name of their choice.   |
| Server IP Address                       | Enter the IP address for the server.  |
| External Port Start                     | Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured. |
| External Port End                       | Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.   |
| Protocol                                | User can select from: TCP, TCP/UDP or UDP.  |
| Internal Port Start                     | Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured  |
| Internal Port End                       | Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.   |

### 6.3.2 Port Triggering

**Note:** This option is not available for Bridge mode.

Some applications require that specific ports in the IAD's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The IAD allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

COMTREND  
**ADSL Router**

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

| Application | Trigger  |            | Open     |            | Remove |
|-------------|----------|------------|----------|------------|--------|
| Name        | Protocol | Port Range | Protocol | Port Range |        |
|             |          | Start End  |          | Start End  |        |

To add a Trigger Port, simply click the Add button. The following will be displayed.

**COMTREND ADSL Router**

**NAT -- Port Triggering**

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.  
 Remaining number of entries that can be configured: 32

Application Name:

☒ Select an application: Select One

☐ Custom application:

Save/Apply

| Trigger Port Start   | Trigger Port End     | Trigger Protocol | Open Port Start      | Open Port End        | Open Protocol |
|----------------------|----------------------|------------------|----------------------|----------------------|---------------|
| <input type="text"/> | <input type="text"/> | TCP              | <input type="text"/> | <input type="text"/> | TCP           |
| <input type="text"/> | <input type="text"/> | TCP              | <input type="text"/> | <input type="text"/> | TCP           |
| <input type="text"/> | <input type="text"/> | TCP              | <input type="text"/> | <input type="text"/> | TCP           |
| <input type="text"/> | <input type="text"/> | TCP              | <input type="text"/> | <input type="text"/> | TCP           |
| <input type="text"/> | <input type="text"/> | TCP              | <input type="text"/> | <input type="text"/> | TCP           |
| <input type="text"/> | <input type="text"/> | TCP              | <input type="text"/> | <input type="text"/> | TCP           |
| <input type="text"/> | <input type="text"/> | TCP              | <input type="text"/> | <input type="text"/> | TCP           |
| <input type="text"/> | <input type="text"/> | TCP              | <input type="text"/> | <input type="text"/> | TCP           |
| <input type="text"/> | <input type="text"/> | TCP              | <input type="text"/> | <input type="text"/> | TCP           |
| <input type="text"/> | <input type="text"/> | TCP              | <input type="text"/> | <input type="text"/> | TCP           |

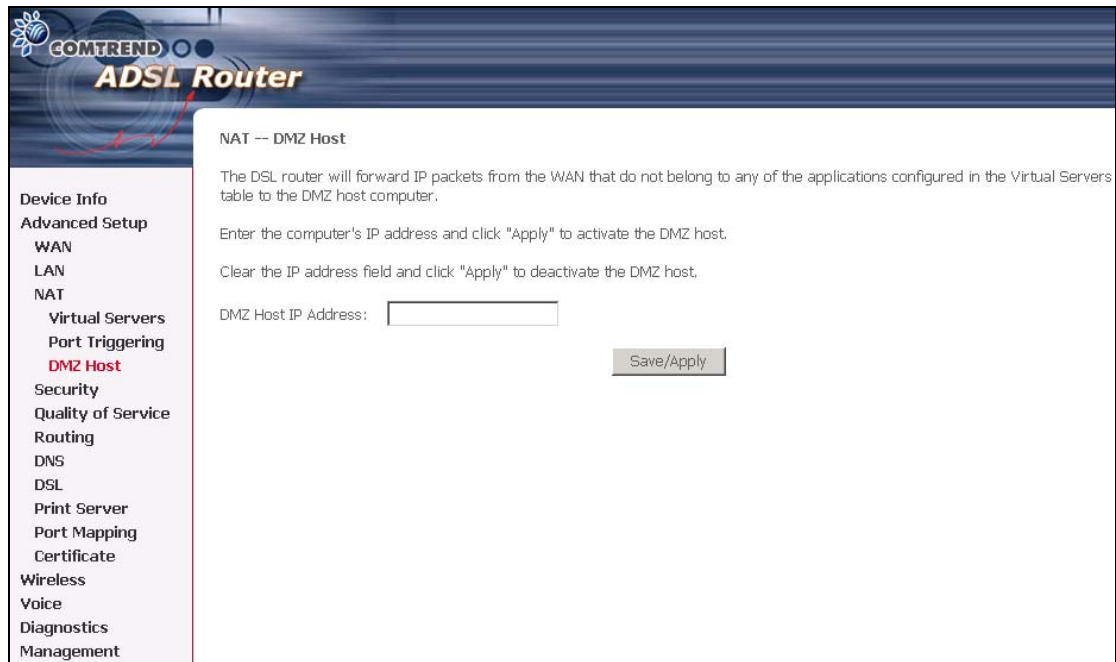
Save/Apply

|   |  |
|---|--|
| Select an Application<br>Or<br>Custom Application | User should select the application from the list.<br>Or<br>User can enter the name of their choice.  |
| Trigger Port Start                                | Enter the starting trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured. |
| Trigger Port End                                  | Enter the ending trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.   |
| Trigger Protocol                                  | User can select from: TCP, TCP/UDP or UDP.   |
| Open Port Start                                   | Enter the starting open port number (when you select custom application). When an application is selected the port ranges are automatically configured.    |
| Open Port End                                     | Enter the ending open port number (when you select custom application). When an application is selected the port ranges are automatically configured.      |
| Open Protocol                                     | User can select from: TCP, TCP/UDP or UDP.   |

### 6.3.3 DMZ Host

**Note:** This option is not available for Bridge mode.

The VoIP IAD will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.



The screenshot shows the Comtrend ADSL Router web interface. On the left is a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Virtual Servers, Port Triggering, DMZ Host (highlighted in red), Security, Quality of Service, Routing, DNS, DSL, Print Server, Port Mapping, Certificate, Wireless, Voice, Diagnostics, and Management. The main content area is titled "NAT -- DMZ Host". It contains the following text: "The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.", "Enter the computer's IP address and click 'Apply' to activate the DMZ host.", and "Clear the IP address field and click 'Apply' to deactivate the DMZ host.". Below this text is a label "DMZ Host IP Address:" followed by a text input field. To the right of the input field is a "Save/Apply" button.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

## 6.4 Security

### 6.4.1 MAC Filtering

Mac Filtering is only available for Bridged mode.

Each network device has a unique MAC address. You can block or forward the packets based on the MAC addresses. The MAC Filtering Setup screen allows setting up the MAC filtering policy and the MAC filtering rules. MAC Filtering is only effective on ATM PVCs configured in Bridge mode.

The policy **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table. The default is FORWARD; you change by clicking the **Change Policy** button.

COMTREND ADSL Router

Device Info  
Advanced Setup  
WAN  
LAN  
Security  
MAC Filtering  
Parental Control  
Quality of Service  
Routing  
DSL  
Print Server  
Port Mapping  
Certificate  
Wireless  
Voice  
Diagnostics  
Management

MAC Filtering Setup

MAC Filtering Global Policy: **FORWARDED**

Change Policy


MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Choose Add or Remove to configure MAC filtering rules.

| VPI/VCI | Protocol | Destination MAC | Source MAC | Frame Direction | Remove |
|---------|----------|-----------------|------------|-----------------|--------|
|---------|----------|-----------------|------------|-----------------|--------|

Add Remove

Choose **Add** or **Remove** to configure MAC filtering rules. The following screen pops up when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click **Apply** to save and activate the filter.



Device Info  
Advanced Setup  
WAN  
LAN  
Security  
MAC Filtering  
Parental Control  
Quality of Service  
Routing  
DSL  
Print Server  
Port Mapping  
Certificate  
Wireless  
Voice  
Diagnostics  
Management

### Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

☒ Select All

☒ br\_0\_35/nas\_0\_35

Save/Apply

| Option                  | Description                                      |
|-------------------------|--|
| Protocol type           | PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP |
| Destination MAC Address | Define the destination MAC address               |
| Source MAC Address      | Define the source MAC address                    |
| Frame Direction         | Select the incoming/outgoing packet interface    |

## 6.4.2 Parental Control

### Daytime Parental Control

This feature restricts access of a selected LAN device to an outside Network through the router, as per chosen days of the week and the chosen times.

COMTREND ADSL Router

Time of Day Restrictions -- A maximum 16 entries can be configured.

| Username | MAC | Mon | Tue | Wed | Thu | Fri | Sat | Sun | Start | Stop | Remove |
|----------|-----|-----|-----|-----|-----|-----|-----|-----|-------|------|--------|
|----------|-----|-----|-----|-----|-----|-----|-----|-----|-------|------|--------|

Add Remove

Click **Add** to display the following screen.

COMTREND ADSL Router

Time of Day Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

☒ Browser's MAC Address 00:05:5D:0C:56:E1  
☐ Other MAC Address   
(xx:xx:xx:xx:xx:xx)

| Days of the week | Mon                      | Tue                      | Wed                      | Thu                      | Fri                      | Sat                      | Sun                      |
|------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Click to select  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Save/Apply

Click Save/Apply to enforce the settings.

**User Name:** Name of the Filter.

**Browser's MAC Address:** Displays MAC address of the LAN device on which the browser is running.

**Other MAC Address:** If restrictions are to be applied to a device other than the one on which the browser is running, the MAC address of that LAN device is entered.

**Days of the Week:** Days of the week, when the restrictions are applied.

**Start Blocking Time:** The time when restrictions on the LAN device are put into effect.

**End Blocking Time:** The time when restrictions on the LAN device are lifted.

### 6.4.3 IP Filtering

This option is not available for bridge mode.

IP filtering allows you to create a filter rule to identify outgoing/incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

**Note:** After you enable the "Firewall", you can set the "IP filter". If firewall is disabled, you cannot set the IP filter.


#### Outgoing

Note: The default setting for all Outgoing traffic is Accepted.

The screenshot shows the COMTREND ADSL Router web interface. On the left is a navigation menu with categories: Device Info, Advanced Setup, Security, Routing, DSL, Print Server, Port Mapping, Certificate, Wireless, Voice, Diagnostics, and Management. Under 'Advanced Setup', 'IP Filtering' is selected, and 'Outgoing' is highlighted in red. The main content area is titled 'Outgoing IP Filtering Setup'. It contains a paragraph: 'By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters. Choose Add or Remove to configure outgoing IP filters.' Below this is a table with the following headers: Filter Name, Protocol, Source Address / Mask, Source Port, Dest. Address / Mask, Dest. Port, and Remove. The table is currently empty. Below the table are two buttons: 'Add' and 'Remove'.

| Filter Name | Protocol | Source Address / Mask | Source Port | Dest. Address / Mask | Dest. Port | Remove |
|-------------|----------|-----------------------|-------------|----------------------|------------|--------|
|-------------|----------|-----------------------|-------------|----------------------|------------|--------|

To add a filtering rule, simply click the Add button. The following screen will be displayed.



**Device Info**  
**Advanced Setup**  
WAN  
LAN  
NAT  
**Security**  
  IP Filtering  
    Outgoing  
    Incoming  
  Parental Control  
Routing  
DNS  
DSL  
Print Server  
Port Mapping  
Certificate  
Wireless  
Voice  
Diagnostics  
Management

### Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

|                                      |  |
|--------------------------------------|--|
| Filter Name                          | Type a name for the filter rule.                 |
| Protocol                             | User can select from: TCP, TCP/UDP, UDP or ICMP. |
| Source IP address                    | Enter source IP address.                         |
| Source Subnet Mask                   | Enter source subnet mask.                        |
| Source Port (port or port:port)      | Enter source port number or port range.          |
| Destination IP address               | Enter destination IP address.                    |
| Destination Subnet Mask              | Enter destination subnet mask.                   |
| Destination port (port or port:port) | Enter destination port number or port range.     |

## Incoming

Note: The default setting for all Incoming traffic is Blocked.

The screenshot shows the 'Incoming IP Filtering Setup' page. On the left is a navigation menu with categories: Device Info, Advanced Setup (WAN, LAN, NAT), Security (IP Filtering, Outgoing, Incoming, Parental Control), Routing, DNS, DSL, Print Server, Port Mapping, Certificate, Wireless, Voice, Diagnostics, and Management. The 'Incoming' option under Security is highlighted. The main content area is titled 'Incoming IP Filtering Setup' and contains the following text: 'By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.' Below this is the instruction 'Choose Add or Remove to configure incoming IP filters.' and a table with the following headers: Filter Name, VPI/VCI, Protocol, Source Address / Mask, Source Port, Dest. Address / Mask, Dest. Port, and Remove. Below the table are 'Add' and 'Remove' buttons.

| Filter Name | VPI/VCI | Protocol | Source Address / Mask | Source Port | Dest. Address / Mask | Dest. Port | Remove |
|-------------|---------|----------|-----------------------|-------------|----------------------|------------|--------|
|-------------|---------|----------|-----------------------|-------------|----------------------|------------|--------|

To add a filtering rule, simply click the Add button. The following screen will be displayed.

The screenshot shows the 'Add IP Filter -- Incoming' page. The left navigation menu is the same as the previous screenshot, with 'Incoming' highlighted. The main content area is titled 'Add IP Filter -- Incoming' and contains the following text: 'The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.' Below this are input fields for: Filter Name, Protocol (a dropdown menu), Source IP address, Source Subnet Mask, Source Port (port or port:port), Destination IP address, Destination Subnet Mask, and Destination Port (port or port:port). Below these fields is a section titled 'WAN Interfaces (Configured in Routing mode and with firewall enabled only)' with the instruction 'Select at least one or multiple WAN interfaces displayed below to apply this rule.' This section contains two checked checkboxes: 'Select All' and 'pppoe\_0\_35\_1/ppp\_0\_35\_1'. At the bottom right is a 'Save/Apply' button.

To configure the parameters, please reference **Outgoing** table above.

## 6.5 Quality of Service

To display the quality of service function, you need to enable the QoS feature in the WAN Setup.

The screenshot shows the 'Quality of Service Setup' page on a COMTREND ADSL Router. The left sidebar contains a menu with options: Device Info, Advanced Setup, WAN, LAN, NAT, Security, Quality of Service (highlighted in red), Routing, DNS, DSL, Print Server, Port Mapping, Certificate, Wireless, Voice, Diagnostics, and Management. The main content area is titled 'Quality of Service Setup' and includes the instruction: 'Choose Add or Remove to configure network traffic classes.' Below this is a table for 'Differentiated Service Configuration'. The table has columns for Class Name, Priority, IP Precedence, IP Type of Service, WAN 802.1P, Lan Port, Protocol, Source Addr./Mask, Source Port, Dest. Addr./Mask, Dest. Port, 802.1P, and Remove. Below the table are 'Add' and 'Remove' buttons.

| MARK       |          |               |                    | TRAFFIC CLASSIFICATION RULES |          |          |                   |             |                  |            |        |        |
|------------|----------|---------------|--------------------|------------------------------|----------|----------|-------------------|-------------|------------------|------------|--------|--------|
|            |          |               |                    | SET-1                        |          |          |                   |             |                  | SET-2      |        |        |
| Class Name | Priority | IP Precedence | IP Type of Service | WAN 802.1P                   | Lan Port | Protocol | Source Addr./Mask | Source Port | Dest. Addr./Mask | Dest. Port | 802.1P | Remove |

Differentiated Service Configuration

| MARK       |          |           |          | TRAFFIC CLASSIFICATION RULES |                   |             |                  |            |                       |                            |        |                |        |
|------------|----------|-----------|----------|------------------------------|-------------------|-------------|------------------|------------|-----------------------|----------------------------|--------|----------------|--------|
| Class Name | Priority | DSCP Mark | Lan Port | Protocol                     | Source Addr./Mask | Source Port | Dest. Addr./Mask | Dest. Port | Source MAC Addr./Mask | Destination MAC Addr./Mask | 802.1P | Enable/Disable | Remove |

Choose Add to configure network traffic classes. The following screen will be displayed:

The screenshot shows the 'Add Network Traffic Class Rule' page on a COMTREND ADSL Router. The left sidebar is the same as the previous screenshot, with 'Quality of Service' highlighted. The main content area is titled 'Add Network Traffic Class Rule' and includes the instruction: 'The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.' Below this is a form with the following fields: Traffic Class Name (text input), Enable Differentiated Service Configuration (checkbox), Assign ATM Priority and/or IP Precedence and/or Type Of Service for the class (text input), Mark IP Precedence (dropdown), Mark IP Type Of Service (dropdown), Mark 802.1p if 802.1q is enabled on WAN (dropdown), Specify Traffic Classification Rules (text input), SET-1 (text input), Physical LAN Port (dropdown), Protocol (dropdown), Source IP Address (text input), Source Subnet Mask (text input), UDP/TCP Source Port (port or port:port) (text input), Destination IP Address (text input), Destination Subnet Mask (text input), UDP/TCP Destination Port (port or port:port) (text input), SET-2 (text input), 802.1p Priority (dropdown), and a 'Save/Apply' button.

Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

Traffic Class Name:

☐ Enable Differentiated Service Configuration

Assign ATM Priority and/or IP Precedence and/or Type Of Service for the class

If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the corresponding TOS byte in the IP header of the upstream packet is overwritten by the selected value.

Note: If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.

Assign ATM Transmit Priority:

Mark IP Precedence:

Mark IP Type Of Service:

Mark 802.1p if 802.1q is enabled on WAN:

Specify Traffic Classification Rules

Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.

SET-1

Physical LAN Port:

Protocol:

Source IP Address:

Source Subnet Mask:

UDP/TCP Source Port (port or port:port):

Destination IP Address:

Destination Subnet Mask:

UDP/TCP Destination Port (port or port:port):

SET-2

802.1p Priority:

|   |   |
|---|---|
| Traffic Class Name                      | Enter name for traffic class.   |
| Assign ATM Transmit Priority            | Select Low, Medium or High.   |
| Mark IP Precedence                      | Select between 0-7. The lower the digit shows the higher the priority.                                  |
| Mark IP Type Of Service                 | Select either: Normal Service, Minimize Cost, Maximize Reliability, Maximize Throughput, Minimize Delay |
| Mark 802.1p if 802.1q is enabled on WAN | Select between 0-7. The higher the digit shows the higher the priority.                                 |
| <b>SET-1</b>                            |   |
| Physical LAN Port                       | Select between ENET(1-4), USB, Wireless and Wireless_Guest.   |
| Protocol                                | User can select from: TCP, TCP/UDP, UDP or ICMP.  |
| Source IP Address                       | Enter the source IP address.  |
| Source Subnet Mask                      | Enter the subnet mask for the source IP address.  |
| Source Port (port or port:port)         | Enter source port number or port range.   |
| Destination IP address                  | Enter destination IP address.   |
| Destination Subnet Mask                 | Enter destination subnet mask.  |
| Destination port (port or port:port)    | Enter destination port number or port range.  |
| <b>SET-2</b>                            |   |
| 802.1p Priority                         | Select between 0-7. The lower the digit shows the higher the priority                                   |

## 6.6 Routing

The Routing dialog box allows you to configure Default gateway, Static Route and RIP.

**Note:** This " RIP " option is not available for Bridge mode.

### 6.6.1 Default Gateway

If '**Enable Automatic Assigned Default Gateway**' checkbox is selected, this IAD will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

**NOTE:** If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the IAD to get the automatic assigned default gateway.



**Note:** This screenshot is based on PPPoE encapsulation.

## 6.6.2 Static Route

Choose **Static Route** to display the Static Route screen. The Static Route screen lists the configured static routes, and allows configuring static routes. Choose **Add** or **Remove** to configure the static routes.

COMTREND ADSL Router

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.

Destination Network Address:

Subnet Mask:

☐ Use Gateway IP Address

☒ Use Interface

Save/Apply

**Note:** This screenshot is based on PPPoE encapsulation.

To add static route, click the **Add** button to display the following screen. Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click **Save/Apply** to add the entry to the routing table.

COMTREND ADSL Router

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.

Destination Network Address:

Subnet Mask:

☐ Use Gateway IP Address

☒ Use Interface

Save/Apply

### 6.6.3 RIP

To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

COMTREND  
**ADSL Router**

Routing -- RIP Configuration

To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

Global RIP Mode ☒ Disabled ☐ Enabled

| Interface  | VPI/VCI | Version | Operation | Enabled                  |
|------------|---------|---------|-----------|--------------------------|
| br0        | (LAN)   | 2       | Active    | <input type="checkbox"/> |
| ppp_0_35_1 | 0/35    | 2       | Passive   | <input type="checkbox"/> |

Save/Apply

**Note:** This screenshot is based on PPPoE encapsulation.

## 6.7 DNS

### 6.7.1 DNS Server

If 'Enable Automatic Assigned DNS' checkbox is selected, this IAD will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the IAD to make the new configuration effective.



The screenshot shows the web interface of a COMTREND ADSL Router. On the left is a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, NAT, Security, Quality of Service, Routing, DNS, **DNS Server** (highlighted in red), Dynamic DNS, DSL, Print Server, Port Mapping, Certificate, Wireless, Voice, Diagnostics, and Management. The main content area is titled 'DNS Server Configuration'. It contains a paragraph explaining the 'Enable Automatic Assigned DNS' checkbox. Below the text is a checkbox labeled 'Enable Automatic Assigned DNS' which is checked. At the bottom right of the main area is a 'Save' button.

**COMTREND ADSL Router**

**DNS Server Configuration**

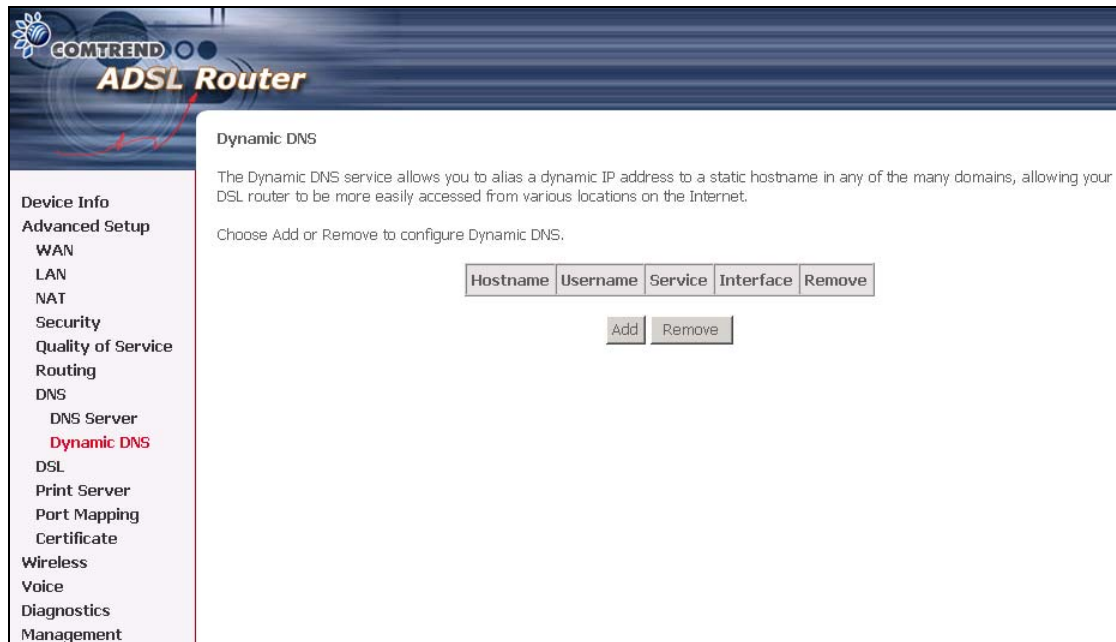
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.

☒ Enable Automatic Assigned DNS


Save

## 6.7.2 Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your VoIP IAD to be more easily accessed from various locations on the Internet.



To add a dynamic DNS service, simply click the Add button. The following screen will be displayed:



**Device Info**

**Advanced Setup**

WAN

LAN

NAT

Security

Quality of Service

Routing

DNS

    DNS Server

    Dynamic DNS

DSL

Print Server

Port Mapping

Certificate

Wireless

Voice

Diagnostics

Management

### Add dynamic DDNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider

Hostname

Interface

**DynDNS Settings**

Username

Password

|                |  |
|----------------|--|
| D-DNS provider | Select a dynamic DNS provider from the list    |
| Hostname       | Enter the name for the dynamic DNS server.     |
| Interface      | Select the interface from the list             |
| Username       | Enter the username for the dynamic DNS server. |
| Password       | Enter the password for the dynamic DNS server. |

## 6.8 DSL

To access the DSL settings, First click On **Advanced Setup** and then click on **DSL**. The DSL Settings dialog box allows you to select an appropriate modulation mode. Note that this means the IAD uses one of the selected modulation modes to sync with the DSLAM if two more modes are selected.

**COMTREND ADSL Router**

**DSL Settings**

Select the modulation mode below.

- ☒ G.Dmt Enabled
- ☒ G.lite Enabled
- ☒ T1.413 Enabled
- ☒ ADSL2 Enabled
- ☒ AnnexL Enabled
- ☒ ADSL2+ Enabled
- ☐ AnnexM Enabled

Select the phone line pair below.

- ☒ Inner pair
- ☐ Outer pair

Capability

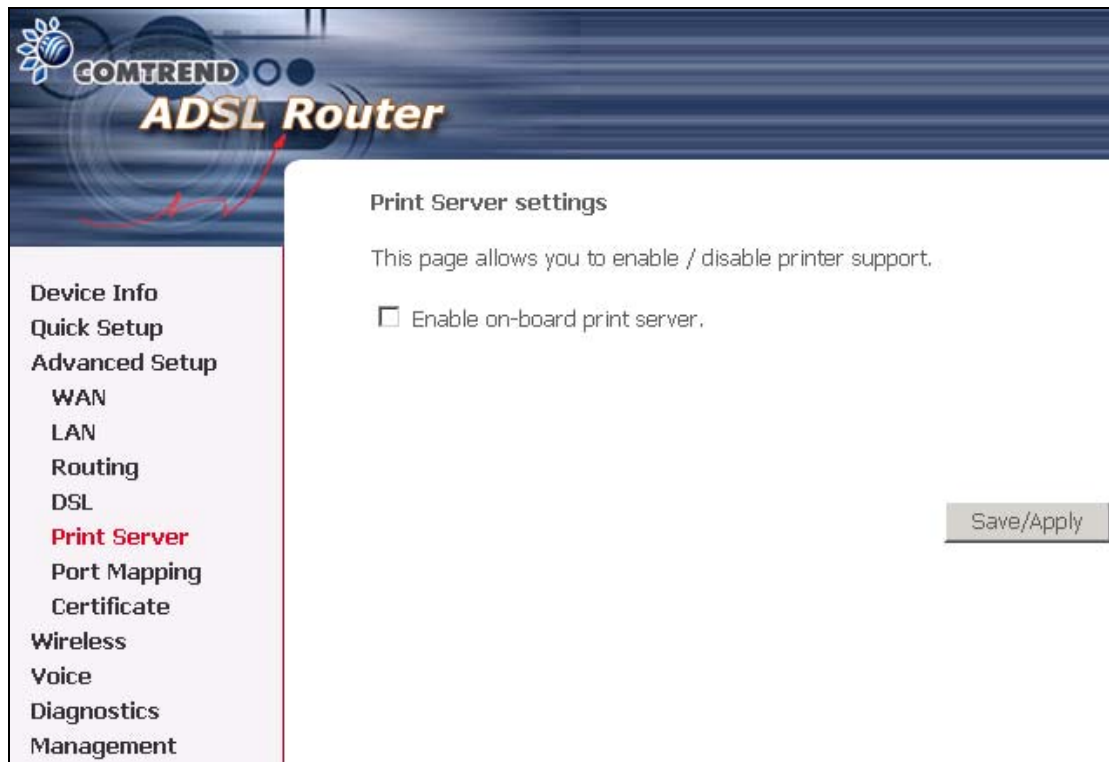
- ☒ Bitswap Enable
- ☐ SRA Enable

Save/Apply

| Option         | Description  |
|----------------|--|
| G.dmt          | Sets G.Dmt if you want the system to use only G.Dmt mode                 |
| G.lite         | Sets G.lite if you want the system to use only G.lite mode               |
| T1.413         | Sets the T1.413 if you want the system to use only T1.413 mode           |
| ADSL2 Enabled  | The device can support the functions of the ADSL2                        |
| AnnexL Enabled | The device can support/enhance the long loop test                        |
| ADSL2+ Enabled | The device can support the functions of the ADSL2+                       |
| AnnexM Enabled | The device can support/enhance the data rate of both upstream/downstream |
| Inner Pair     | Reserved only  |
| Outer Pair     | Reserved only  |
| Bitswap Enable | Allows bitswaping function   |
| SRA Enable     | Allows seamless rate adaptation  |

## 6.9 Print Server

The CT-6382D is equipped with one high-speed USB2.0 host connection. With software support, users can connect USB devices such as a printer and hard disc to the CT-6382D. For this software release, printer server is supported.



Please refer to Appendix A for an Example.

## 6.10 Port Mapping

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group.

As shown below, when you tick the Enable virtual ports on, all of the LAN interfaces will be grouped together as a default.

COMTREND ADSL Router

Device Info  
Quick Setup  
Advanced Setup  
WAN  
LAN  
Routing  
DSL  
Print Server  
**Port Mapping**  
Certificate  
Wireless  
Voice  
Diagnostics  
Management

Port Mapping -- A maximum 16 entries can be configured

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

☐ Enable virtual ports on

| Group Name | Interfaces                               | Remove | Edit |
|------------|--|--------|------|
| Default    | ENET(1-4), USB, Wireless, Wireless_Guest |        |      |

Port Mapping -- A maximum 16 entries can be configured

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

☒ Enable virtual ports on

| Group Name | Interfaces  | Remove | Edit |
|------------|---|--------|------|
| Default    | ENET1, ENET2, ENET3, ENET4, USB, Wireless, Wireless_Guest |        |      |

To add a port mapping group, simply click the Add button.

**COMTREND ADSL Router**

**Port Mapping Configuration**

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.  
**Note that these clients may obtain public IP addresses**
3. Click Save/Apply button to make the changes effective immediately

**Note that the selected interfaces will be removed from their existing groups and added to the new group.**

**IMPORTANT** If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

| Grouped Interfaces  | Available Interfaces   |
|---|--|
| <div style="border: 1px solid black; height: 60px; width: 100%;"></div> | ENET1<br>ENET2<br>ENET3<br>ENET4<br>USB<br>Wireless<br>Wireless_Gues |

Automatically Add Clients With the following DHCP Vendor IDs

To create a group from the list, first enter the group name and then select from the available interfaces on the list.

### **Automatically Add Clients With the Following DHCP Vendor IDs:**

Add support to automatically map LAN interfaces including Wireless and USB to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when PortMapping is enabled.

There are 4 PVCs (0/33, 0/36, 0/37, 0/38). 0/33 is for PPPoE and the others are for IP setup-box (video).

The Lan interfaces are ETH1, ETH2, ETH3, ETH4, Wireless and USB.  
Port mapping configuration are:

1. Default : ENET1, ENET2, ENET3, ENET4, Wireless, Wireless\_Guest and USB.
2. Video: nas\_0\_36, nas\_0\_37 and nas\_0\_38. The DHCP vendor ID is "Video".

The CPE's dhcp server is running on "Default". And ISP's dhcp server is running on PVC 0/36. It is for setup-box use only.

In the LAN side, PC can get IP address from CPE's dhcp server and access Internet via PPPoE (0/33).

If the setup-box was connected with interface "ENET1" and send a dhcp request with vendor id "Video", CPE's dhcp server will forward this request to ISP's dhcp server.

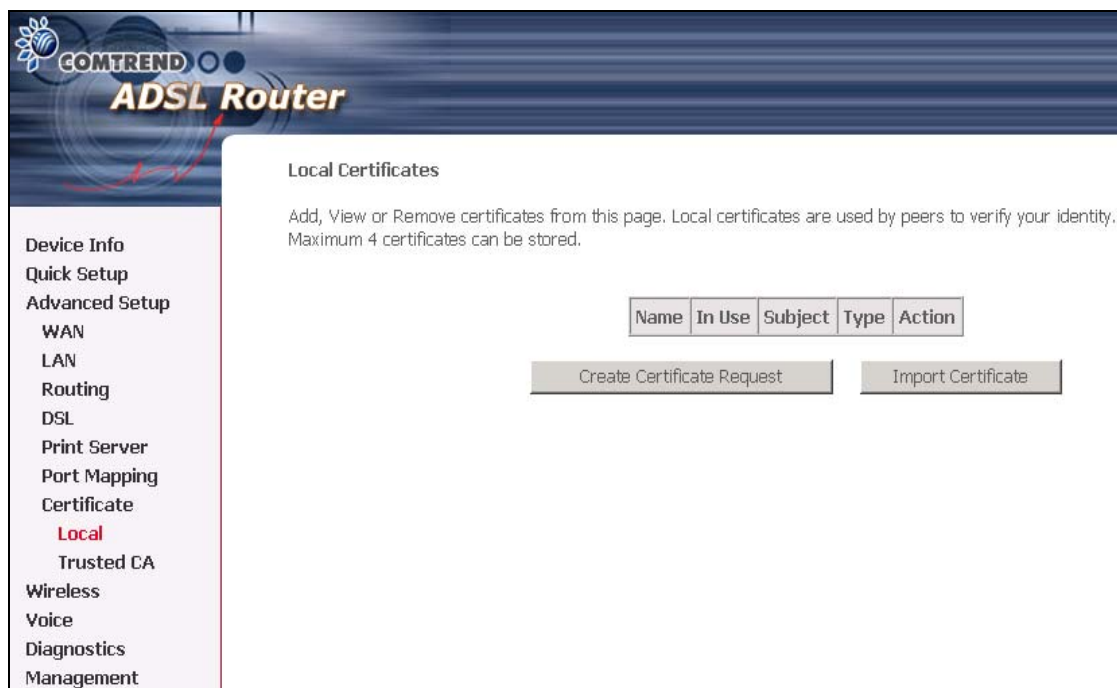
And CPE will change the portmapping configuration automatically. The portmapping configuration will become:

1. Default : ENET2, ENET3, ENET4, Wireless, Wireless\_Guest and USB.
2. Video: nas\_0\_36, nas\_0\_37, nas\_0\_38 and ENET1.

## 6.11 Certificate

A certificate is a public key, attached with its owner's information (company name, server name, personal real name, contact e-mail, postal address, etc) and digital signatures. There will be one or more digital signatures attached on the certificate, indicating that these signers have verified that the owner information of this certificate is correct.

### 6.11.1 Local



Click **Create Certificate Request** to generate a certificate signing request. The certificate signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate signing request. Actually, your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. The explanation for each column in the following table is only for reference.

|                     |   |
|---------------------|---|
| Certificate Name    | A user-defined name for the certificate.  |
| Common Name         | Usually, it is the fully qualified domain name for the machine.                     |
| Organization Name   | The exact legal name of your organization. Do not abbreviate.                       |
| State/Province Name | The state or province where your organization is located. It cannot be abbreviated. |
| Country/Region Name | The two-letter ISO abbreviation for your country.                                   |

**COMTREND ADSL Router**

**Create new certificate request**

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

Country/Region Name:

Click **Apply** to generate a private key and a certificate signing request.

This page is used to paste the certificate content and the private key provided by your vendor/ISP/ITSP.



Device Info

Quick Setup

Advanced Setup

WAN

LAN

Routing

DSL

Print Server

Port Mapping

Certificate

Local

Trusted CA

Wireless

Voice

Diagnostics

Management

Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

-----BEGIN CERTIFICATE-----

<insert certificate here>

-----END CERTIFICATE-----

Private Key:

-----BEGIN RSA PRIVATE KEY-----

<insert private key here>

-----END RSA PRIVATE KEY-----

Apply

## 6.11.2 Trusted CA

CA is the abbreviation for Certificate Authority. CA is a part of the X.509 system. It is itself a certificate, attached with the owner information of this certificate authority. But its purpose is not to do encryption/decryption. Its purpose is to sign and issue certificates; in order to prove the owner information of that certificate is correct.

The screenshot shows the 'Trusted CA (Certificate Authority) Certificates' page in the COMTREND ADSL Router web interface. The left sidebar contains a menu with options: Device Info, Quick Setup, Advanced Setup, WAN, LAN, Routing, DSL, Print Server, Port Mapping, Certificate, Local, **Trusted CA**, Wireless, Voice, Diagnostics, and Management. The main content area has a title 'Trusted CA (Certificate Authority) Certificates' and a description: 'Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.' Below this is a table with headers 'Name', 'Subject', 'Type', and 'Action'. An 'Import Certificate' button is located below the table.

Click **Import Certificate** to paste the certificate content of your trusted CA. Generally speaking, the certificate content will be provided by your vendor/ISP/ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.

The screenshot shows the 'Import CA certificate' page in the COMTREND ADSL Router web interface. The left sidebar contains a menu with options: Device Info, Advanced Setup, WAN, LAN, NAT, Security, Quality of Service, Routing, DNS, DSL, Print Server, Port Mapping, IPsec, Certificate, Local, Trusted CA, Wireless, Diagnostics, and Management. The main content area has a title 'Import CA certificate' and a description: 'Enter certificate name and paste certificate content.' Below this is a form with two fields: 'Certificate Name:' and 'Certificate:'. The 'Certificate Name' field is a text input. The 'Certificate' field is a large text area containing the placeholder text: '-----BEGIN CERTIFICATE-----<br><insert certificate here><br>-----END CERTIFICATE-----'. An 'Apply' button is located at the bottom right of the form.

# Chapter 7 Wireless

The Wireless dialog box allows you to enable the wireless capability, hide the access point, set the wireless network name and restrict the channel set.

The screenshot shows the 'Wireless -- Basic' configuration page of a Comtrend ADSL Router. The left sidebar contains a menu with options: Device Info, Quick Setup, Advanced Setup, Wireless (highlighted), Basic (highlighted with a red box), Security, MAC Filter, Wireless Bridge, Advanced, Quality of Service, Station Info, Voice, Diagnostics, and Management. The main content area is titled 'Wireless -- Basic' and includes a description: 'This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply" to configure the basic wireless options.' Below this, there are several configuration options: 'Enable Wireless' (checked), 'Hide Access Point' (unchecked), 'SSID' (text field with 'Comtrend'), 'BSSID' (text field with '00:16:38:CC:E3:0F'), 'Country' (dropdown menu with 'UNITED STATES'), 'Enable Wireless Guest Network' (unchecked), and 'Guest SSID' (text field with 'Guest'). A 'Save/Apply' button is located at the bottom right.

## 7.1 Wireless Basic Screen

The Basic option allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.

Click **Apply** to configure the basic wireless options.

This screenshot is identical to the one above, showing the 'Wireless -- Basic' configuration page of a Comtrend ADSL Router. The left sidebar menu is the same, with 'Wireless' and 'Basic' highlighted. The main content area contains the same configuration options: 'Enable Wireless' (checked), 'Hide Access Point' (unchecked), 'SSID' (text field with 'Comtrend'), 'BSSID' (text field with '00:16:38:CC:E3:0F'), 'Country' (dropdown menu with 'UNITED STATES'), 'Enable Wireless Guest Network' (unchecked), and 'Guest SSID' (text field with 'Guest'). A 'Save/Apply' button is at the bottom right.

| Option            | Description  |
|-------------------|--|
| Enable Wireless   | A checkbox that enables or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, and County settings. The default is Enable Wireless.   |
| Hide Access Point | <p>Select Hide Access Point to protect VoIP IAD access point from detection by wireless active scans. If you do not want the access point to be automatically detected by a wireless station, this checkbox should be de-selected.</p> <p>The station will not discover this access point. To connect a station to the available access points, the station must manually add this access point name in its wireless configuration.</p> <p>In Windows XP, go to the Network&gt;Programs function to view all of the available access points. You can also use other software programs such as NetStumbler to view available access points.</p> |
| SSID              | <p>Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.</p> <p>The naming conventions are: Minimum is one character and maximum number of characters: 32 bytes.</p>   |
| BSSID             | The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.  |
| Country           | <p>A drop-down menu that permits worldwide and specific national settings. Each county listed in the menu enforces specific regulations limiting channel range:</p> <ul style="list-style-type: none"> <li>● US= worldwide</li> <li>● Japan=1-14</li> <li>● Jordan= 10-13</li> <li>● Israel= TBD</li> </ul>  |

## 7.1.1 Security

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The system that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then sends back a frame that indicates whether it recognizes the identity of the sending station.

Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from 802.11 wireless network communications channel.

The following screen appears when Security is selected. The Security page allows you to configure security features of the wireless LAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.



The screenshot shows the 'Wireless -- Security' configuration page of a Comtrend ADSL Router. The page has a dark blue header with the 'COMTREND ADSL Router' logo. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Wireless (selected), Basic, Security (highlighted in red), MAC Filter, Wireless Bridge, Advanced, Quality of Service, Station Info, Voice, Diagnostics, and Management. The main content area is titled 'Wireless -- Security' and contains a descriptive paragraph: 'This page allows you to configure security features of the wireless LAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply" to configure the wireless security options.' Below this are three configuration fields: 'Select SSID:' with a dropdown menu showing 'Comtrend', 'Network Authentication:' with a dropdown menu showing 'Open', and 'WEP Encryption:' with a dropdown menu showing 'Disabled'. A 'Save/Apply' button is located at the bottom right of the configuration area.

Click **Apply** to configure the wireless security options.

| Option                 | Description   |
|------------------------|---|
| Network Authentication | <p>It specifies the network authentication. When this checkbox is selected, it specifies that a network key be used for authentication to the wireless network. If the Network Authentication (Shared mode) checkbox is not shared (that is, if open system authentication is used), no authentication is provided. Open system authentication only performs identity verifications.</p> <p>Different authentication type pops up different settings requests.</p> <p>Choosing <b>802.1X</b>, enter RADIUS Server IP address, RADIUS Port, RADIUS key and Current Network Key.</p> <p>Also, enable WEP Encryption and select Encryption Strength.</p> <div> <p>Select SSID: Comtrend</p> <p>Network Authentication: 802.1X</p> <p>RADIUS Server IP Address: 0.0.0.0</p> <p>RADIUS Port: 1812</p> <p>RADIUS Key:</p> <p>WEP Encryption: Enabled</p> <p>Encryption Strength: 128-bit</p> <p>Current Network Key: 2</p> <p>Network Key 1:</p> <p>Network Key 2:</p> <p>Network Key 3:</p> <p>Network Key 4:</p> <p>Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys<br/>Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys</p> <p>Save/Apply</p> </div> <p>Select the Current Network Key and enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys and enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.</p> |

|                     |  |
|---------------------|--|
|                     | <p>Choosing <b>WPA</b>, you must enter WPA Group Rekey Interval.</p> <div> <div>Select SSID: Comtrend</div> <div>Network Authentication: WPA</div> <div>WPA Group Rekey Interval: 0</div> <div>RADIUS Server IP Address: 0.0.0.0</div> <div>RADIUS Port: 1812</div> <div>RADIUS Key:</div> <div>WPA Encryption: TKIP</div> <div>WEP Encryption: Disabled</div> <div>Save/Apply</div> </div> <p>Choosing <b>WPA-PSK</b>, you must enter WPA Pre-Shared Key and Group Rekey Interval.</p> <div> <div>Select SSID: Comtrend</div> <div>Network Authentication: WPA-PSK</div> <div>WPA Pre-Shared Key: <a href="#">Click here to display</a></div> <div>WPA Group Rekey Interval: 0</div> <div>WPA Encryption: TKIP</div> <div>WEP Encryption: Disabled</div> <div>Save/Apply</div> </div> |
| WEP Encryption      | <p>It specifies that a network key is used to encrypt the data is sent over the network. When this checkbox is selected, it enables data encryption and prompts the Encryption Strength drop-down menu. Data Encryption (WEP Enabled) and Network Authentication use the same key.</p>   |
| Encryption strength | <p>A session's key strength is proportional to the number of binary bits comprising the session key file. This means that session keys with a greater number of bits have a greater degree of security, and are considerably more difficult to forcibly decode. This drop-down menu sets either a 64 8-bit (5-character or 10-character hexadecimal or 128 8-bit (13-character or 10-character) key.</p> <p>If you set a minimum 128-bit key strength, users attempting to establish a secure communications channel with your server must use a browser capable of communicating with a 128-bit session key.</p> <p>The Encryption Strength settings do not display unless the network Authentication (shared Mode) check box is selected.</p>  |

## 7.1.2 MAC Filter

This MAC Filter page allows access to be restricted/allowed based on a MAC address. All NICs have a unique 48-bit MAC address burned into the ROM chip on the card. When MAC address filtering is enabled, you are restricting the NICs that are allowed to connect to your access point. Therefore, an access point will grant access to any computer that is using a NIC whose MAC address is on its “allows” list.

Wi-Fi IAD's and access points that support MAC filtering let you specify a list of MAC addresses that may connect to the access point, and thus dictate what devices are authorized to access the wireless network. When a device is using MAC filtering, any address not explicitly defined will be denied access.

MAC Restrict mode: **Off** - disables MAC filtering; **Allow** – permits **access** for the specified MAC address; deny; reject access of the specified MAC address, then click the **SET** button.

To delete an entry, select the entry at the bottom of the screen and then click the **Remove** button, located on the right hand side of the screen.

To add a MAC entry, click **Add** and enter MAC address



After choosing the Add button, the following screen appears. Enter the MAC address and click **Apply** to add the MAC address to the wireless MAC address filters.

COMTREND ADSL Router

Wireless -- MAC Filter

Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.

MAC Address:

Device Info  
Quick Setup  
Advanced Setup  
Wireless  
Basic  
Security  
MAC Filter  
Wireless Bridge  
Advanced  
Quality of Service  
Station Info  
Voice  
Diagnostics  
Management

COMTREND ADSL Router

Wireless -- MAC Filter

MAC Restrict Mode: ☒ Disabled ☐ Allow ☐ Deny

| MAC Address       | Remove                   |
|-------------------|--------------------------|
| AB:0A:00:12:12:AB | <input type="checkbox"/> |

Device Info  
Quick Setup  
Advanced Setup  
Wireless  
Basic  
Security  
MAC Filter  
Wireless Bridge  
Advanced  
Quality of Service  
Station Info  
Voice  
Diagnostics  
Management

| Option            | Description   |
|-------------------|---|
| MAC Restrict Mode | Radio buttons that allow settings of;<br>Off: MAC filtering function is disabled.<br>Allow: Permits PCs with listed MAC addresses to connect to the access point.<br>Deny: Prevents PCs with listed MAC from connecting to the access point.  |
| MAC Address       | Lists the MAC addresses subject to the Off, Allow, or Deny instruction. The Add button prompts an entry field that requires you type in a MAC address in a two-character, 6-byte convention: xx:xx:xx:xx:xx:xx where xx are hexadecimal numbers. The maximum number of MAC addresses that can be added is 60. |

### 7.1.3 Wireless Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict, which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

**COMTREND ADSL Router**

**Wireless -- Bridge**

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Save/Apply" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

| Option          | Description     |
|-----------------|-----------------|
| AP Mode         | Access Point    |
|                 | Wireless Bridge |
| Bridge Restrict | Enabled         |
|                 | Enabled (Scan)  |
|                 | Disabled        |

## 7.1.4 Advanced

The Advanced page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point and set whether short or long preambles are used. Click **Apply** to configure the advanced wireless options.

**COMTREND ADSL Router**

**Wireless -- Advanced**

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click "Apply" to configure the advanced wireless options.

AP Isolation:

Band:

Channel:

Rate:

Multicast Rate:

Basic Rate:

Fragmentation Threshold:

RTS Threshold:

DTIM Interval:

Beacon Interval:

XPress™ Technology:

54g™ Mode:

54g Protection:

Afterburner Technology:

WMM(Wi-Fi Multimedia):

| Option       | Description   |
|--------------|---|
| AP Isolation | Select On or Off. By enabling this feature, wireless clients associated with the Access Point will be able to connect to each other.  |
| Band         | The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.) |

|                          |  |
|--------------------------|--|
| Channel                  | Drop-down menu that allows selection of specific channel   |
| Auto Channel Timer (min) | Auto channel scan timer in minutes (0 to disable)  |
| 54g™ Rate                | Drop-down menu that specifies the following fixed rates:<br>Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary.<br>1 Mbps, 2Mbps, 5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.  |
| Multicast Rate           | Setting multicast packet transmit rate   |
| Basic Rate               | Setting basic transmit rate  |
| Fragmentation Threshold  | A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented.<br>Enter a value between 256 and 2346.<br>If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346.<br>Setting the Fragmentation Threshold too low may result in poor performance. |
| RTS Threshold            | Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS.<br>The default setting of 2347 (maximum length) disables RTS Threshold.   |

|                    |  |
|--------------------|--|
| DTIM Interval      | <p>Delivery Traffic Indication Message (DTIM), also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.</p>  |
| Beacon Interval    | <p>The amount of time between beacon transmissions. Each beacon transmission identifies the presence of an access point. By default, radio NICs passively scan all RF channels and listen for beacons coming from access points to find a suitable access point.</p> <p>Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).</p> <p>The entered value is represented in ms. Default is 100. Acceptable entry range is 1 to 0xffff (65535)</p> |
| Xpress™ Technology | <p>Xpress Technology is compliant with draft specifications of two planned wireless industry standards.</p>  |
| 54g™ Mode          | <p>Select the mode to 54g Auto for the widest compatibility. Select the mode to 54g Performance for the fastest performance among 54g certified equipment. Set the mode to 54g LRS if you are experiencing difficulty with legacy 802.11b equipment.</p>   |
| 54g Protection     | <p>In Auto mode the IAD will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.</p>   |

|                |  |
|----------------|--|
| Preamble Type  | <p>Short preamble is intended for application where maximum throughput is desired but it doesn't cooperate with the legacy.</p> <p>Long preamble interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999</p> |
| Transmit Power | The router will set different power output (by percentage) according to this selection.  |

### 7.1.5 Quality of Service

WMM provides advanced quality of service (QoS) features for Wi-Fi networks to improve the end-user experience by prioritizing audio, video and voice traffic and optimizing the way shared network resources are allocated among competing applications.



If you want to enable Click on the drop down menu and select, then click the **Save/Apply WME Settings** button.

### 7.1.6 Station Info

This page shows authenticated wireless stations and their status.

**Wireless -- Authenticated Stations**

This page shows authenticated wireless stations and their status.

| BSSID             | Associated | Authorized |
|-------------------|------------|------------|
| 00:12:F0:B5:C9:9C |            |            |

Refresh

**Device Info**  
**Quick Setup**  
**Advanced Setup**  
**Wireless**  
    Basic  
    Security  
    MAC Filter  
    Wireless Bridge  
    Advanced  
    Quality of Service  
    **Station Info**  
Voice  
Diagnostics  
Management

|            |   |
|------------|---|
| BSSID      | The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly. |
| Associated | Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.   |
| Authorized | Lists those devices with authorized access.   |

## Chapter 8 Voice

SIP, the Session Initiation Protocol, is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. It is the Internet Engineering Task Force's (IETF's) standard for multimedia conferencing over IP. It is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

Session Initiation Protocol is a peer-to-peer protocol. There are four components in SIP standard, (a) User Agent (UA), (b) Proxy Server, (c) Registrar Server, and, (d) Redirect Server. This particular document describes about SIP User Agent and the call establishment between User Agents.

To access SIP, Simply click on the Voice->**SIP** from main menu. The following screen will be displayed.

## 8.1 SIP

**COMTREND ADSL Router**

**Voice -- SIP configuration**

Enter the SIP parameters and click Start/Stop to save the parameters and start/stop the voice application.

Interface name:

Locale selection:

Preferred codec:

Preferred ptime:

☒ Use SIP Proxy.

SIP Proxy:

SIP Proxy port:

Register Expire Time:

SIP domain name:

☐ Use SIP Outbound Proxy.

☒ Enable SIP tag matching (Uncheck for Vonage Interop).

☐ Remote server for SIP log messages.

|                                       | DispName:                         | VoIP Phone Number:                | Auth. ID:            | Auth. Password:      |
|---------------------------------------|-----------------------------------|-----------------------------------|----------------------|----------------------|
| 1 <input checked="" type="checkbox"/> | <input type="text" value="1001"/> | <input type="text" value="1001"/> | <input type="text"/> | <input type="text"/> |
| 2 <input checked="" type="checkbox"/> | <input type="text" value="2001"/> | <input type="text" value="2001"/> | <input type="text"/> | <input type="text"/> |
| 3 <input checked="" type="checkbox"/> | <input type="text" value="3001"/> | <input type="text" value="3001"/> | <input type="text"/> | <input type="text"/> |
| 4 <input checked="" type="checkbox"/> | <input type="text" value="4001"/> | <input type="text" value="4001"/> | <input type="text"/> | <input type="text"/> |

| Line:  | FXS 1  | FXS 2  | DECT 1                                       | DECT 2                                       |
|--------|--|--|--|--|
| Group: | <input type="text" value="Account 1 Group"/> | <input type="text" value="Account 2 Group"/> | <input type="text" value="Account 3 Group"/> | <input type="text" value="Account 4 Group"/> |

PSTN route rule:

Emergency calls : Number: 1.  2.

FAX mode:

Max Digits:

RFC2833 Outband DTMF:

RTP Payload Type for RFC2833:

Once the settings are configured click **Stop SIP client** to stop the VoIP service and to start click **Start SIP client** to run the new configuration.

|                 |   |
|-----------------|---|
| Interface name  | WAN interface name  |
| Local Selection | Set tone, ring type and physical characteristics for each specific country. |

|   |  |
|---|--|
| Preferred codec   | The preferred codec of this user. The default is G.711U first.   |
| Preferred ptime   | The preferred ptime of this user. The default is 20.   |
| Use SIP proxy   | <p>A proxy is an intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or transferred to other servers. A proxy interprets and, if necessary, rewrites a request message before forwarding it.</p> <p>Input IP address or domain name of the SIP proxy server, used for VOIP service. 5060 is the default (change based on your VoIP service provider).</p> |
| Register Expire Time  | The time period until user would like its registration to be valid with the Registrar/Proxy Server. The default value is 300 seconds.  |
| SIP domain name   | Provided by your VoIP service provider.  |
| Use SIP outbound proxy<br>Enable SIP tag matching (Uncheck for Vonage Interop). | Click if required by your VoIP service provider.   |
| Remote server for SIP log messages  | Enable or disable log the SIP message to remote server.  |
| DispName  | The string for called party's telephone to display the caller name.  |
| VoIP Phone Number   | Endpoint telephone number. As the modem has two FXS, you can enter two telephone numbers for VoIP phone.   |
| Auth. ID  | The authentication user name for the Registrar/proxy, which is assigned by the service provider.   |
| Auth. Password  | The authentication password for the Registrar/proxy, which is assigned by the service provider.  |

|                                 |  |
|---------------------------------|--|
| SIP Grouping                    | Used to map which account to which line you require.<br>FXS 1 and FXS 2 are phone ports 1 and 2.<br>DECT 1 and DECT2 are DECT line 1 and DECT line 2.  |
| PSTN route rule                 | If PSTN route rule is "auto" , when a PSTN call coming will ring the idle phone(phone1 idle ring phone1,phone1 busy ring phone2)<br><br>If PSTN route rule is "fix", when a PSTN call coming will ring the phone that the user selects from PSTN route data (phone1, phone2 or both) |
| Emergency calls<br>Number 1 & 2 | Emergency phone numbers. <b>Note</b> that you need to change these numbers to correspond with the emergency numbers that are used in your country.   |
| FAX mode:                       | Use G711u (Pass-through) or T.38 when sending a fax.   |
| Max Digits                      | Setup the maximum number of digits for the phone number.   |
| RFC2833 Outband DTMF            | Enable the special use of RTP packets to transmit digit events.  |
| RTP Payload Type for RFC2833    | Payload types are defined in RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals. A payload type is a number from 96 to 127 that identifies the type of payload carried in the packet. The payload type should be identical on the GW and call agent.       |

### 8.1.1 Making Telephone Calls

To make a call, simply dial the number. The dial plan (i.e. the dialed digits) is normally customized for each installation. The default dial plan delivered by Comtrend allows dialing of 4-digit extensions or direct IP addresses. Shorter extension numbers (e.g. 3-digits) can be dialed by completing the dial string with a final #.

When a Call Server (SIP Proxy Server) is configured into the system, the dialed digits are translated and routed by the Call Server to the correct destination as registered with the Call Server.

If no Call Server is configured, calls can still be made using 4-digit extensions, rather than using full IP addresses. The originator translates the dialed-digits to a destination device as follows:

- First digit: line identifier (for multi-line gateways)
- Remaining digits: Host number part of an IP address. The Network number part is considered to be the same as the caller's IP address.

For example, if a caller at address 10.136.64.33/24 dials "2023", the call will be placed to the second line at address 10.136.64.23. All devices have to be on the same Class C subnet (24 bit subnet mask).

To dial an IP address directly, dial the IP address digits, using keypad \* as the dot. Complete the address with a final \* or #. When using IP address dialing it is not possible to specify which line at a gateway is called, so the gateway always routes IP-address dialed calls to the first line.

Network busy tone (fast busy) will be played for unknown or unreachable destinations.

To answer calls, simply pick up the phone or press the handsfree button.

**Caller ID**

The Call Manager delivers Calling Number when placing calls. The calling number is transmitted to the analog line for CLASS recognition.

**Call Hold**

To put a call on hold, press flash then hang up (optional). To return to the original call, press flash or pick up the phone. The phone will issue a short ring burst every 30 seconds or so while on-hook to remind you that a call is on hold.

**Call Transfer**

To transfer a call, press flash then dial the new number.

To transfer immediately, hang up (blind transfer).

To transfer with consultation, wait for the party to answer, consult, and then hang up.

To abort the transfer (if the third party does not answer), press flash to return to the original call.

**Conference Calling**

To turn a two-party call into a three-party conference call, press flash and dial the third party. Wait for the party to answer, then press flash.

To drop the third party and return to a two-party call, press flash again. To drop yourself out of the conference, hang up. The call will be transferred (so that the other two parties remain connected to each other). In conference mode, the conference initiator performs the audio bridge/mixing function – there are only 2 voice streams established.

**Call Waiting**

If call waiting is enabled on a line (see feature codes), and you hear the call waiting tone during a call, press flash to answer the second call. The first call is automatically placed on hold. To switch between calls, press flash again.

To disable the call waiting feature, dial \*60.

To enable the call waiting feature, dial \*61.

Call forward feature settings (Busy or All) takes priority over the call waiting feature.

Call waiting feature is ignored on new incoming calls if there is already a call on hold or in conference.

**Call Forward Number**

To set the call forward number, dial \*74 then the number. Note that this does not actually enable forwarding; to do so, select the call forward action as described below.

To disable all call forwarding features, dial \*70

**Call Forward No Answer**

To enable call forward on no answer, dial \*71. Incoming calls will be forward if unanswered for 18 seconds.

**Call Forward Busy**

To enable call forward if busy, dial \*72. Incoming calls will be immediately forwarded if the phone is off-hook.

**Call Forward All**

To enable call forward for all calls, dial \*73.

To disable the "forward all calls" feature, dial \*75. Previous settings for Call Forward Busy or No Answer are not modified.

**Call Return**


To place a call to the last known incoming caller (unanswered or not), dial \*69.

**Redial**

To redial the last outgoing number, dial \*68.

## 8.2 DECT

Please refer to pages 8 and 9 for details.



Device Info  
Advanced Setup  
Wireless  
Voice  
SIP  
**DECT**  
Diagnostics  
Management

### Voice -- DECT configuration

Enter the DECT parameters and click Apply to set DECT device.

|                  |         |
|------------------|---------|
| Dect HW Version: | 2       |
| Dect SW Version: | 8       |
| PIN Code:        | 0 7 2 3 |

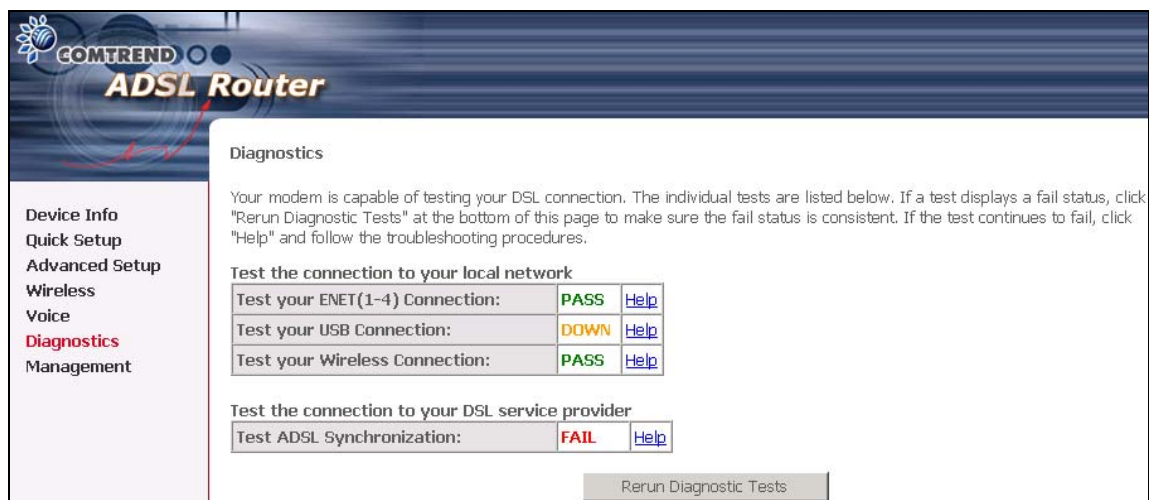
|                     |      |
|---------------------|------|
| Dect Line 1 Status: | Idle |
| Dect Line 2 Status: | Idle |

  
Trunk Line 1 Gain Level: Tx:  Rx:   
Trunk Line 2 Gain Level: Tx:  Rx:   
  
Register Mode:    

| Phone No | Register state | Deregister               | Dect Line 1                         | Dect Line 2                         |
|----------|----------------|--------------------------|-------------------------------------|-------------------------------------|
| 1        | Empty          | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| 2        | Empty          | <input type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| 3        | Empty          | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| 4        | Empty          | <input type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| 5        | Empty          | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |

## Chapter 9 Diagnostics

The Diagnostics menu provides feedback on the connection status of the CT-6382D and the ADSL link. The individual tests are listed below. If a test displays a fail status, click **Rerun Diagnostic Tests** at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click **Help** and follow the troubleshooting procedures.



| Test                | Description   |
|---------------------|---|
| Ethernet Connection | <p><b>Pass:</b> indicates that the Ethernet interface from your computer is connected to the LAN port of your VoIP IAD. A flashing or solid green LAN LED on the IAD also signifies that an Ethernet connection is present and that this test is successful.</p> <p><b>Fail:</b> Indicates that the VoIP IAD does not detect the Ethernet interface on your computer.</p> |
| USB connection      | <p><b>Pass:</b> Indicates that the USB interface from your computer is connected to the LAN port of your VoIP IAD.</p> <p><b>Down:</b> Indicates that the VoIP IAD does not detect the USB interface on your computer.</p>  |
| Wireless connection | <p><b>Pass:</b> Indicates that the Wireless interface from your computer is connected to the wireless network.</p> <p><b>Down:</b> Indicates that the VoIP IAD does not detect the wireless network.</p>  |

|                             |   |
|-----------------------------|---|
| <p>ADSL Synchronization</p> | <p><b>Pass:</b> Indicates that the DSL modem has detected a DSL signal from the telephone company. A solid ADSL LED on the IAD also indicates the detection of a DSL signal from the telephone company.</p> <p><b>Fail:</b> indicates that the DSL modem does not detect a signal from the telephone company's DSL network. The ADSL LED will turn off.</p> |
|-----------------------------|---|

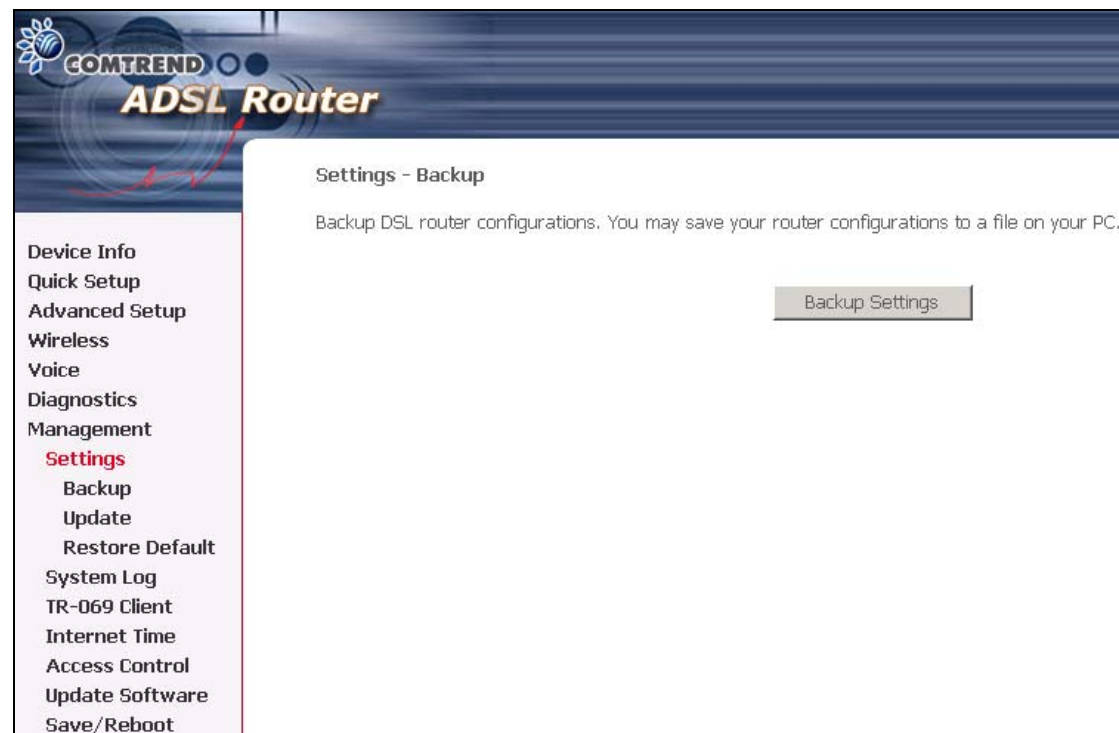
## Chapter 10 Management

The Management section of the CT-6382D supports the following maintenance functions and processes:

- Settings
- System log
- TR-069 Client
- Internet Time
- Access Control
- Update software
- Save/Reboot

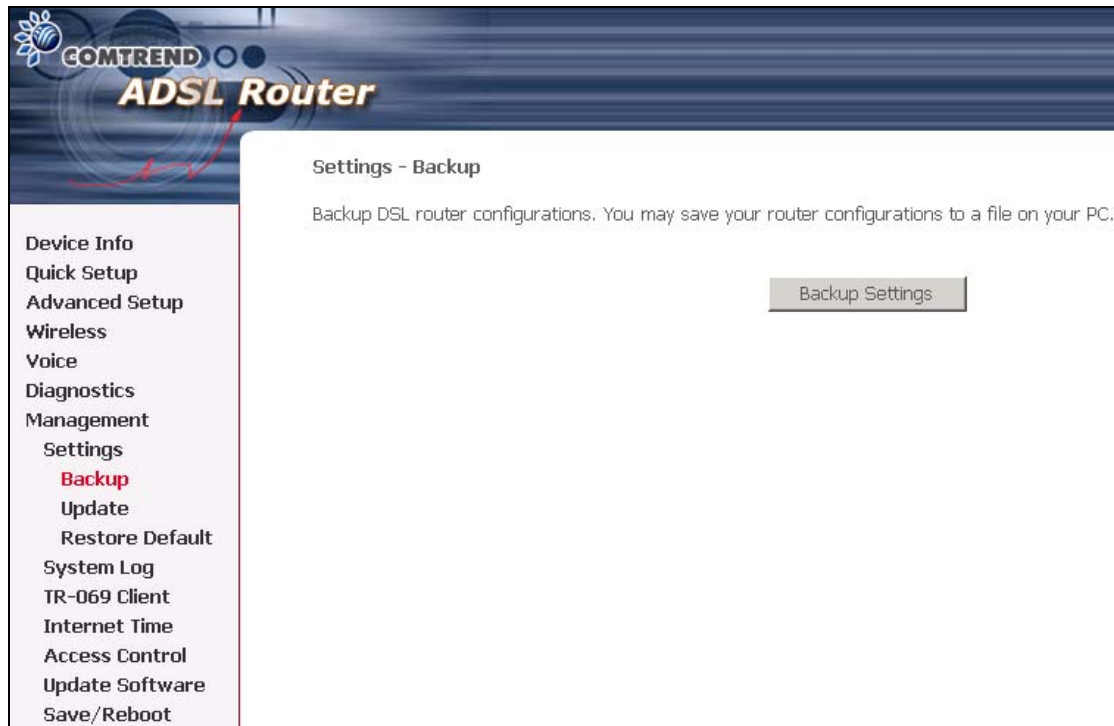
### 10.1 Settings

The Settings option allows you to back up your settings to a file, retrieve the setting file, and restore the settings.



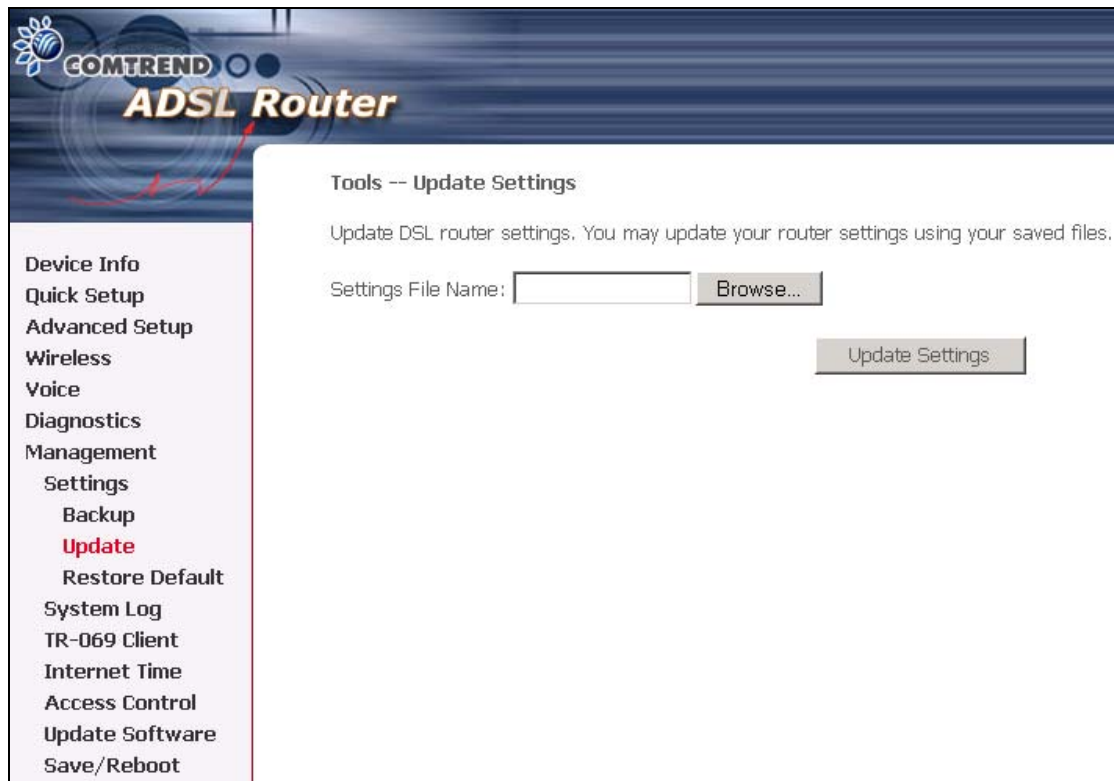
### 10.1.1 Configuration Backup

The Backup option under Management>Settings saves your IAD configurations to a file on your PC. Click Backup Settings in the main window. You will be prompted to define the location of the backup file to save. After choosing the file location, click **Backup Settings**. The file will then be saved to the assigned location.



## 10.1.2 Configuration Restoration

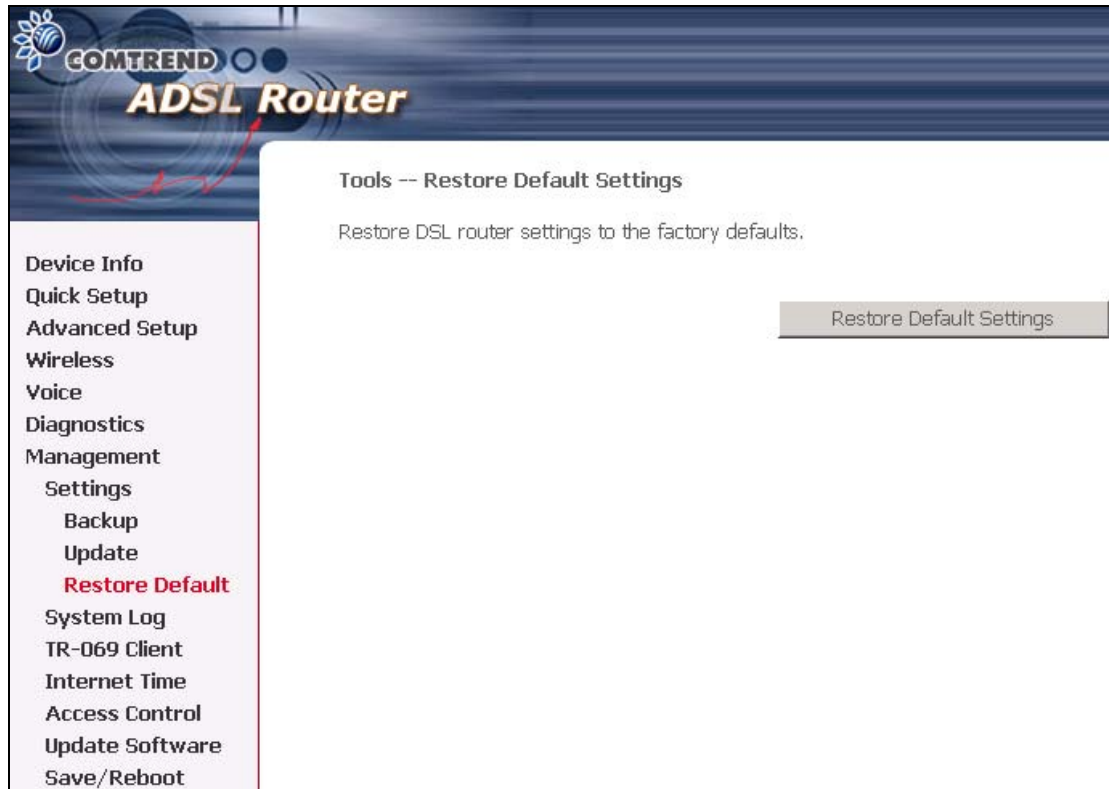
The Update option under Management>Settings update your IAD settings using your saved files.



The screenshot displays the Comtrend ADSL Router web interface. The header features the Comtrend logo and the text 'ADSL Router'. A left-hand navigation menu lists various settings categories: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, Management, Settings, Backup, Update (highlighted in red), Restore Default, System Log, TR-069 Client, Internet Time, Access Control, Update Software, and Save/Reboot. The main content area is titled 'Tools -- Update Settings' and contains the instruction: 'Update DSL router settings. You may update your router settings using your saved files.' Below this, there is a 'Settings File Name:' label followed by a text input field and a 'Browse...' button. At the bottom right of the main area is an 'Update Settings' button.

### 10.1.3 Restore Default

Clicking the Restore Default Configuration option in the Restore Settings screen can restore the original factory installed settings.



**NOTE:** This entry has the same effect as the hardware reset-to-default button. The CT-6382D board hardware and the boot loader support the **reset to default** button. If the reset button is continuously pushed for more than 5 seconds, the boot loader will erase the entire configuration settings saved on the flash memory.

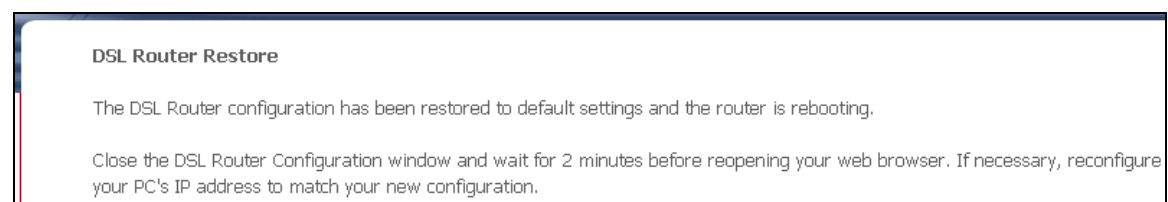
**NOTE:** Restoring system settings require a system reboot. This necessitates that the current Web UI session be closed and restarted. Before restarting the connected PC must be configured with a static IP address in the 192.168.1.x subnet in order to configure the CT-6382D.

## Default settings

The CT-6382D default settings are

- LAN port IP= 192.168.1.1, subnet mask = 255.255.255.0
- Local user name: root
- Password: 12345
- Remote user name: support
- Remote user password: support

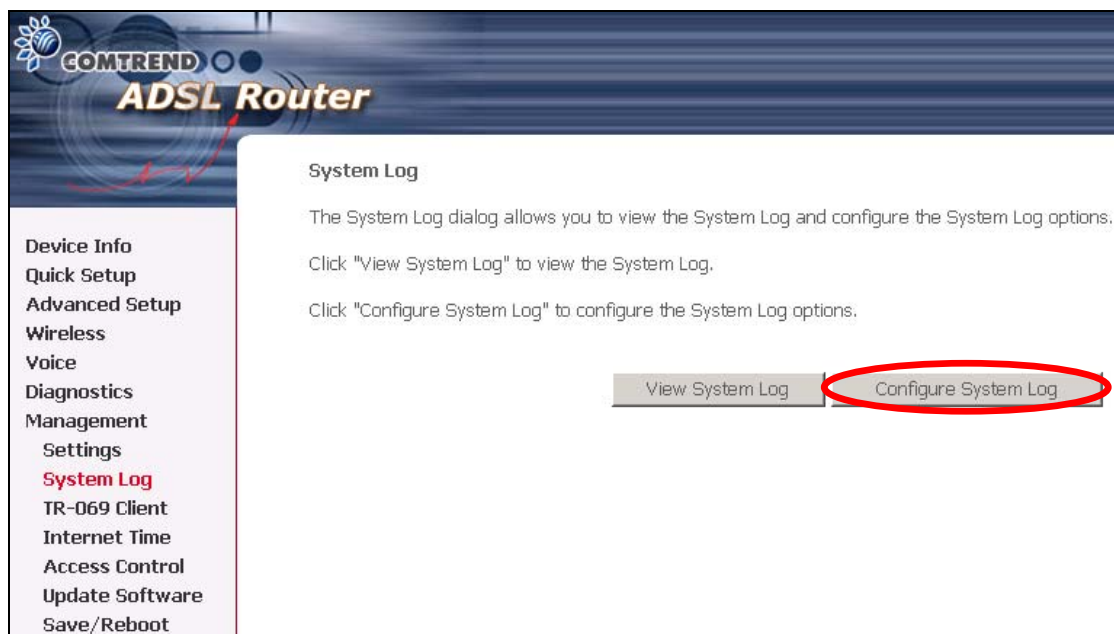
After the Restore Default Configuration button is selected, the following screen appears. Close the VoIP IAD Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.



## 10.2 System Log

The System Log option under Management allows you to view the system events log, or to configure the System Log options. The default setting of system log is enabled. Follow the steps below to enable and view the system log.

1. Click **Configure System Log** to display the following screen.
2. Select from the desired Log options described in the following table, and then click **SAVE/Apply**.



| Option    | Description  |
|-----------|--|
| Log       | Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, tick Enable and then Apply button.   |
| Log level | Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the CT-6382D SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging," which is the lowest critical level. The following log levels are |

|               |  |
|---------------|--|
|               | <ul style="list-style-type: none"> <li>● Emergency = system is unstable</li> <li>● Alert = action must be taken immediately</li> <li>● Critical = critical conditions</li> <li>● Error = Error conditions</li> <li>● Warning = normal but significant condition</li> <li>● Notice</li> <li>● Informational</li> <li>● Debugging = debug-level messages</li> </ul> <p>Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.</p> |
| Display Level | Allows the user to select the logged events and displays on the <b>View System Log</b> page for events of this level and above to the highest Emergency level.   |
| Mode          | <p>Allows you to specify whether events should be stored in the local memory, or be sent to a remote syslog server, or both simultaneously.</p> <p>If remote mode is selected, view system log will not be able to display events saved in the remote syslog server.</p> <p>When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.</p>  |

3. Click **View System Log**. The results are displayed as follows.

| System Log     |          |          |                       |
|----------------|----------|----------|-----------------------|
| Date/Time      | Facility | Severity | Message               |
| Jan 1 00:00:12 | kern     | crit     | kernel: eth0 Link UP. |
| Refresh        |          | Close    |                       |

## 10.3 TR-069 Client

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

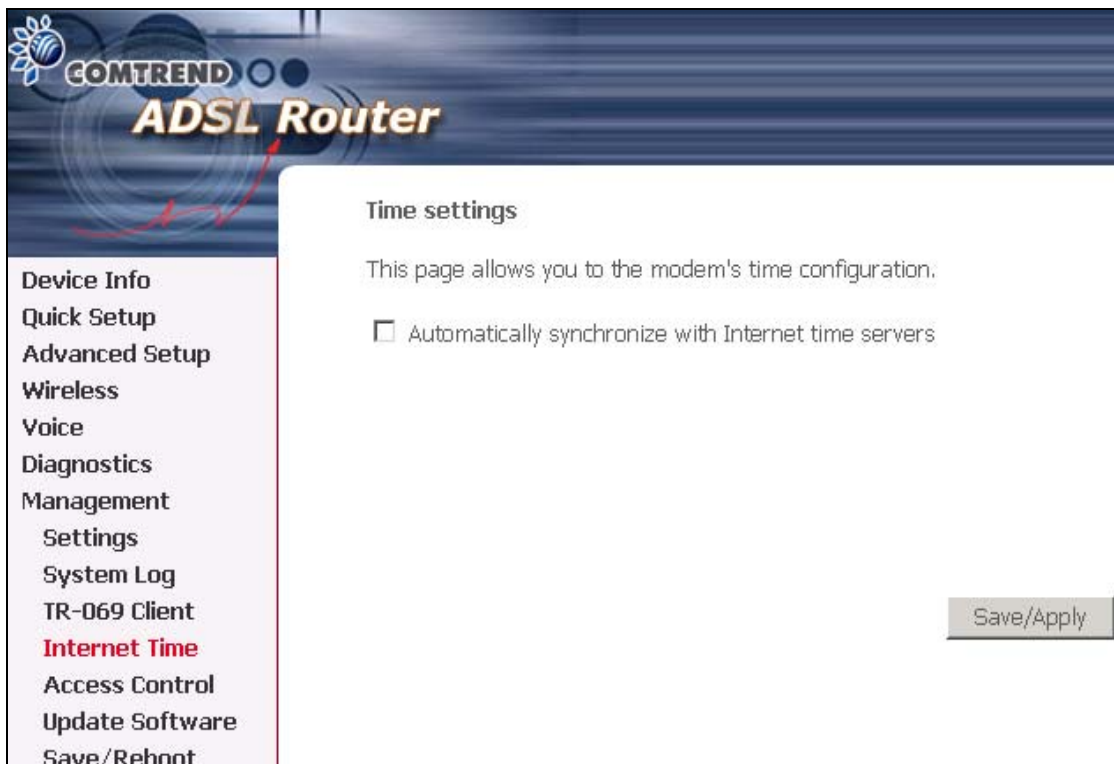
The screenshot shows the 'TR-069 client - Configuration' page of a COMTREND ADSL Router. The left sidebar contains a menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, Management, Settings, System Log, TR-069 Client (highlighted in red), Internet Time, Access Control, Update Software, and Save/Reboot. The main content area has a title 'TR-069 client - Configuration' and a description: 'WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.' Below this, it says 'Select the desired values and click "Apply" to configure the TR-069 client options.' There are three radio buttons: 'Inform' (selected), 'Disable', and 'Enable'. Below these are six input fields: 'Inform Interval' (300), 'ACS URL' (empty), 'ACS User Name' (admin), 'ACS Password' (masked with asterisks), 'Connection Request User Name' (admin), and 'Connection Request Password' (masked with asterisks). At the bottom right are two buttons: 'Save/Apply' and 'GetRPCMethods'.

| Option          | Description  |
|-----------------|--|
| Inform          | Disable/Enable TR-069 client on the CPE.   |
| Inform Interval | The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.   |
| ACS URL         | URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication. |
| ACS User Name   | Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.  |
| ACS Password    | Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.  |

|                                 |   |
|---------------------------------|---|
| Connection Request<br>User Name | Username used to authenticate an ACS making a Connection.<br>Request to the CPE.  |
| Connection Request<br>Password  | Password used to authenticate an ACS making a Connection<br>Request to the CPE.   |
| Get RPC Methods                 | This method may be used by a CPE or ACS to discover the set of methods supported by the ACS or CPE it is in communication with. This list may include both standard TR-069 methods (those defined in this specification or a subsequent version) and vendor-specific methods. The receiver of the response MUST ignore any unrecognized methods. Click this button to force the CPE to immediately establish a connection to the ACS. |

## 10.4 Internet Time

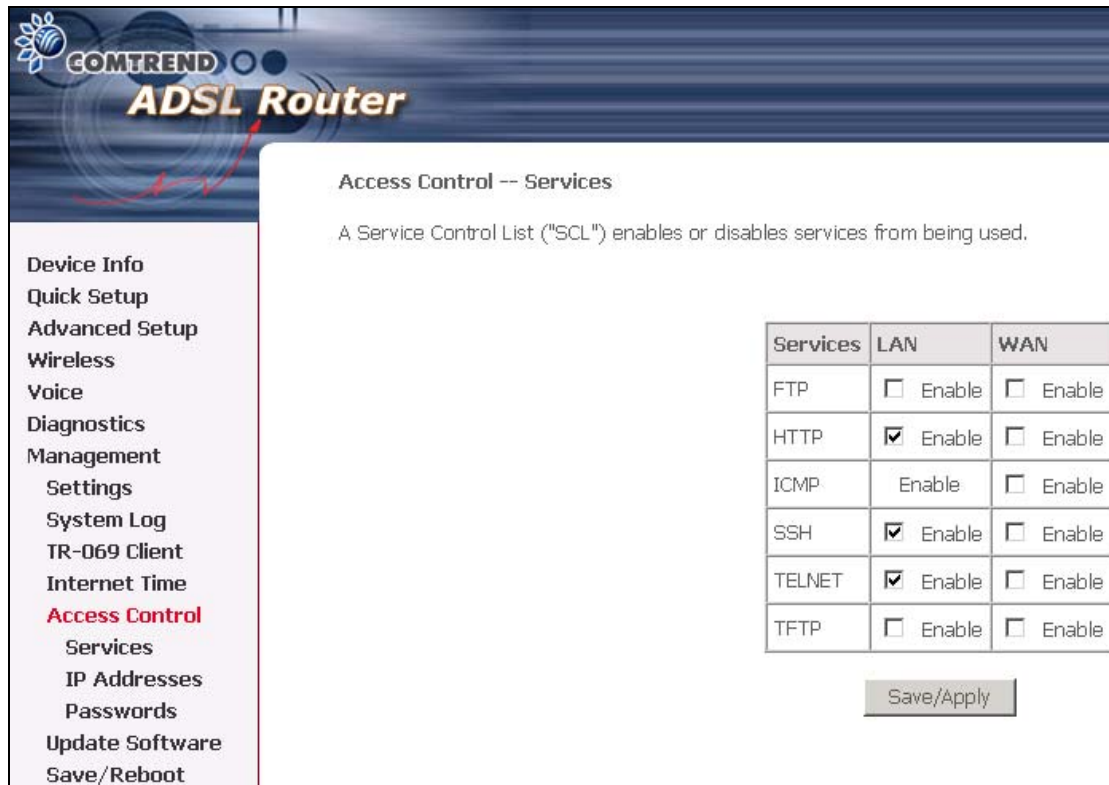
The Internet Time option under Management menu bar configures the Modem's time. To automatically synchronize with Internet timeservers, tick the corresponding box displayed on the screen. Then click **Save/Apply**.



The screenshot shows the web interface of a COMTREND ADSL Router. The top banner features the COMTREND logo and the text "ADSL Router". On the left, a vertical menu lists various configuration options: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, Management, Settings, System Log, TR-069 Client, **Internet Time** (highlighted in red), Access Control, Update Software, and Save/Reboot. The main content area is titled "Time settings" and contains the text "This page allows you to the modem's time configuration." Below this text is a checkbox labeled "Automatically synchronize with Internet time servers", which is currently unchecked. A "Save/Apply" button is located in the bottom right corner of the main content area.

## 10.5 Access Control

The Access Control option under Management menu bar configures the access-related parameters, including three parts: Services, IP Address, and Passwords.



The screenshot displays the Comtrend ADSL Router web interface. The left sidebar contains a navigation menu with the following items: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, Management, Settings, System Log, TR-069 Client, Internet Time, Access Control (highlighted in red), Services, IP Addresses, Passwords, Update Software, and Save/Reboot. The main content area is titled "Access Control -- Services" and includes a description: "A Service Control List ('SCL') enables or disables services from being used." Below this is a table with three columns: Services, LAN, and WAN. The table lists seven services: FTP, HTTP, ICMP, SSH, TELNET, and TFTP. Each service has checkboxes for enabling or disabling it on the LAN and WAN interfaces. The LAN column for HTTP, SSH, and TELNET shows the "Enable" checkbox checked. The WAN column for all services shows the "Enable" checkbox unchecked. A "Save/Apply" button is located at the bottom right of the table.

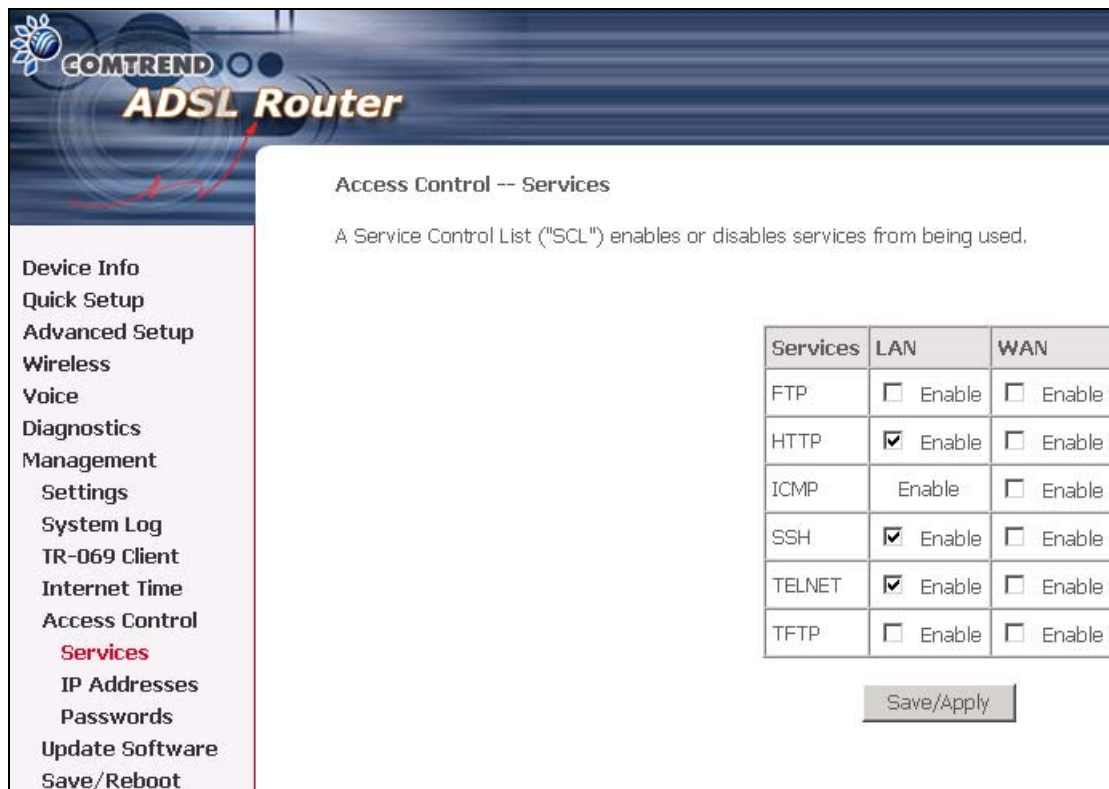
| Services | LAN  | WAN                             |
|----------|--|---------------------------------|
| FTP      | <input type="checkbox"/> Enable            | <input type="checkbox"/> Enable |
| HTTP     | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| ICMP     | <input type="checkbox"/> Enable            | <input type="checkbox"/> Enable |
| SSH      | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| TELNET   | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| TFTP     | <input type="checkbox"/> Enable            | <input type="checkbox"/> Enable |

Save/Apply

## 10.5.1 Services

The Services option limits or opens the access services over the LAN or WAN.

These services are provided FTP, HTTP, ICMP, SSH (Security Socket Share), TELNET, and TFTP. Enable the service by checking the item in the corresponding checkbox, and then click **Save/Apply**.



**COMTREND ADSL Router**

**Access Control -- Services**

A Service Control List ("SCL") enables or disables services from being used.

| Services | LAN  | WAN                             |
|----------|--|---------------------------------|
| FTP      | <input type="checkbox"/> Enable            | <input type="checkbox"/> Enable |
| HTTP     | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| ICMP     | <input type="checkbox"/> Enable            | <input type="checkbox"/> Enable |
| SSH      | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| TELNET   | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable |
| TFTP     | <input type="checkbox"/> Enable            | <input type="checkbox"/> Enable |

**Device Info**  
**Quick Setup**  
**Advanced Setup**  
**Wireless**  
**Voice**  
**Diagnostics**  
**Management**  
  **Settings**  
  System Log  
  TR-069 Client  
  Internet Time  
  Access Control  
  **Services**  
  IP Addresses  
  Passwords  
  Update Software  
  Save/Reboot

## 10.5.2 Access IP Addresses

The IP Addresses option limits the access by IP address. If the Access Control Mode is enabled, only the allowed IP addresses can access the IAD. Before you enable it, configure the IP addresses by clicking the **Add** button. Enter the IP address and click **Apply** to allow the PC with this IP address managing the VoIP IAD.



The screenshot displays the web interface of a COMTREND ADSL Router. The left sidebar contains a navigation menu with the following items: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, Management, Settings, System Log, TR-069 Client, Internet Time, Access Control, Services, **IP Addresses** (highlighted in red), Passwords, Update Software, and Save/Reboot. The main content area is titled "Access Control -- IP Address". It includes a descriptive paragraph: "The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List". Below this text, the "Access Control Mode" is set to "Disable" (indicated by a selected radio button). There are two rows of buttons: the first row has "IP Address" and "Remove" buttons, and the second row has "Add" and "Remove" buttons.

### 10.5.3 Passwords

The Passwords option configures the access passwords for the IAD. Access to your VoIP IAD is controlled through three user accounts: admin, support, and user.

- "root" has unrestricted access to change and view configuration of your VoIP IAD.
- "support" is used to allow an ISP technician to access your VoIP IAD for maintenance and to run diagnostics.
- "user" can access the IAD, view configuration settings and statistics, as well as, update the IAD's software.

Use the fields below to enter up to 16 characters and click Apply to change or create passwords.

The screenshot shows the Comtrend ADSL Router web interface. The header features the Comtrend logo and the text "ADSL Router". A left sidebar contains a navigation menu with the following items: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, Management, Settings, System Log, TR-069 Client, Internet Time, Access Control, Services, IP Addresses, Passwords (highlighted in red), Update Software, and Save/Reboot. The main content area is titled "Access Control -- Passwords". It contains the following text: "Access to your DSL router is controlled through three user accounts: root, support, and user.", "The user name 'root' has unrestricted access to change and view configuration of your DSL Router.", "The user name 'support' is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.", "The user name 'user' can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.", and "Use the fields below to enter up to 16 characters and click 'Apply' to change or create passwords. Note: Password cannot contain a space." Below this text are four input fields: "Username:" (a dropdown menu), "Old Password:", "New Password:", and "Confirm Password:". A "Save/Apply" button is located at the bottom right of the form area.

## 10.6 Update software

The Update Software screen allows you to obtain an updated software image file from your ISP. Manual software upgrades from a locally stored file can be performed using the following screen.



The screenshot shows the 'Update Software' page of a Comtrend ADSL Router. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Wireless, Voice, Diagnostics, Management, Settings, System Log, TR-069 Client, Internet Time, Access Control, **Update Software** (highlighted in red), and Save/Reboot. The main content area is titled 'Tools -- Update Software' and contains the following instructions:

- Step 1:** Obtain an updated software image file from your ISP.
- Step 2:** Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
- Step 3:** Click the "Update Software" button once to upload the new image file.

A note states: 'NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.' Below the instructions, there is a text input field labeled 'Software File Name:' followed by a 'Browse...' button. At the bottom right of the main area is a large 'Update Software' button.

**Step 1:** Obtain an updated software image file from your ISP.

**Step 2:** Enter the path to the image file location in the box below or click the **Browse** button to locate the image file.

**Step 3:** Click the "Update Software" button once to upload the new image file.

**NOTE:** The update process takes about 2 minutes to complete, and your VoIP IAD will reboot.

## 10.7 Save and Reboot

The Save/Reboot options saving the configurations and reboot the IAD. Close the VoIP IAD Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.



## Table A: Encapsulation Mode – Options Table

| <i>Mode</i>          | <b>Mer</b> | <b>IPoA</b> | <b>PPPoA</b> | <b>PPPoE</b> | <b>Bridge</b> | <b>Section</b> |
|----------------------|------------|-------------|--------------|--------------|---------------|----------------|
| <b>WAN</b>           | *          | *           | *            | *            | *             | 6.1            |
| <b>LAN</b>           | *          | *           | *            | *            | *             | 6.2            |
| <b>NAT</b>           |            |             |              |              |               | 6.3            |
| Virtual Servers      | *          | *           | *            | *            |               | 6.3.1          |
| Port Triggering      | *          | *           | *            | *            |               | 6.3.2          |
| DMZ Host             | *          | *           | *            | *            |               | 6.3.3          |
| <b>Security</b>      |            |             |              |              |               | 6.4            |
| IP Filtering         |            |             | *            | *            |               | 6.4.3          |
| <b>QOS</b>           | *          | *           | *            | *            | *             | 6.5            |
| <b>Routing</b>       |            |             |              |              |               | 6.6            |
| Default Gateway      | *          | *           | *            | *            | *             | 6.6.1          |
| Static Route         | *          | *           | *            | *            | *             | 6.6.2          |
| RIP                  | *          | *           | *            | *            |               | 6.6.3          |
| <b>Mac Filtering</b> |            |             |              |              | *             | 6.4.1          |
| <b>DNS</b>           |            |             |              |              |               | 6.7            |
| Dns Server           | *          | *           | *            | *            |               | 6.7.1          |
| Dynamic Dns          | *          | *           | *            | *            |               | 6.7.2          |

Depending on which encapsulation mode you choose, the Advanced menu displayed will vary. Shown here is a table listing the Advanced options for each encapsulation mode.

# Appendix A: Printer Server Configuration

## 1. Introduction

This application notes explain the steps of enabling the Printer Server function in CT-6382D reference platforms.

## 2. How to enable on-board Printer Server function

Following are the steps to enable the on-board Printer Server.

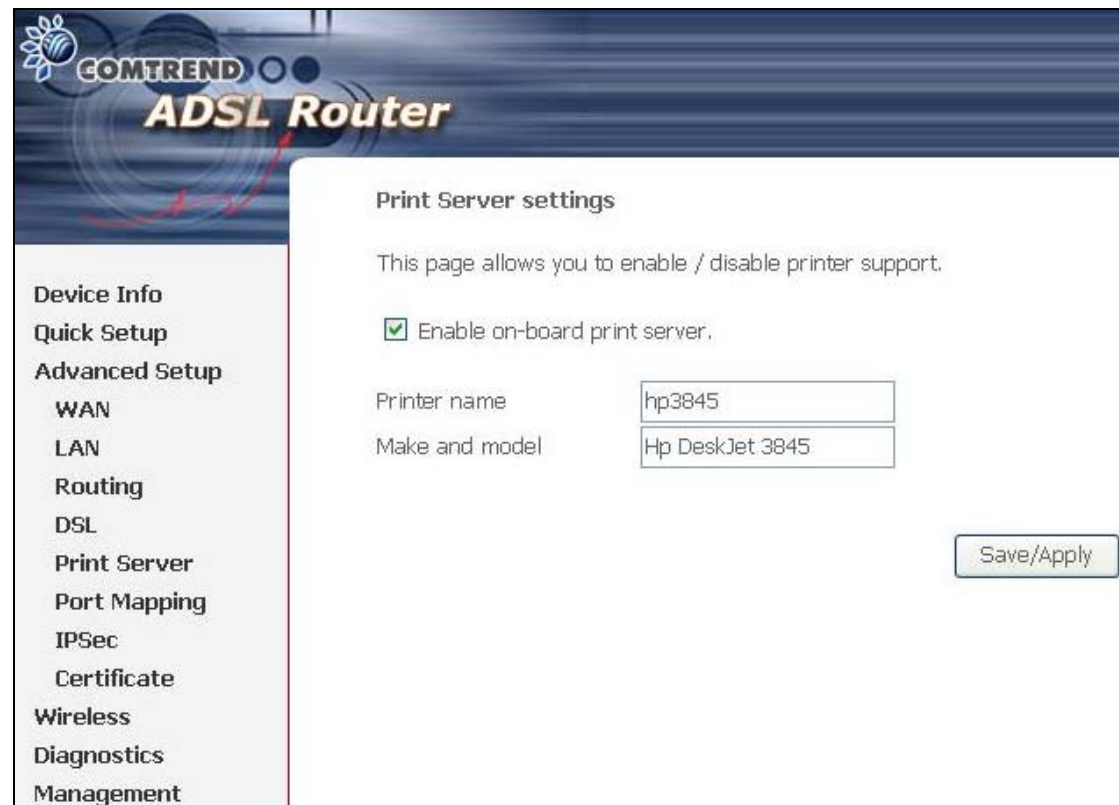
**Step1:** Enable Print Server from Modem Web GUI.

Check **"Enable on-board printer server"** and key in **"Printer name"**, **"Make and model"**

### Note:

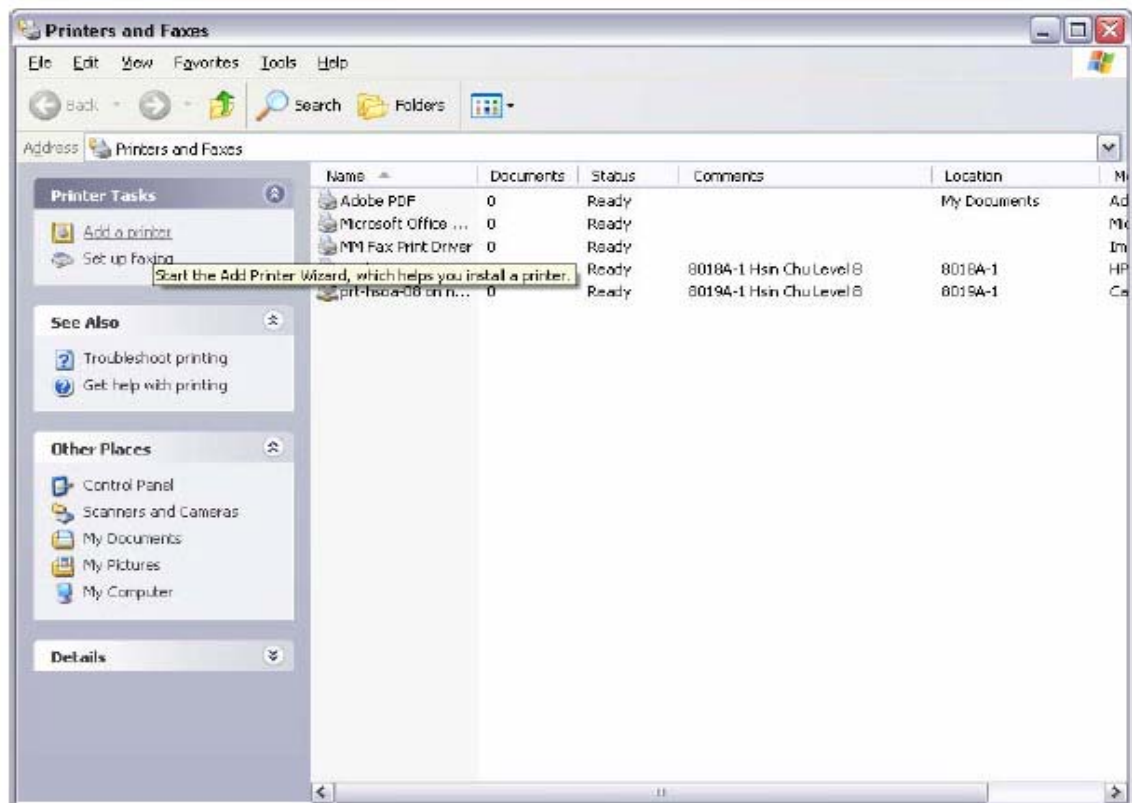
The **"Printer name"** can be any text string up to 40 characters.

The **"Make and model"** can be any text string up to 128 characters.



The screenshot displays the Comtrend ADSL Router Web GUI. On the left is a navigation menu with the following items: Device Info, Quick Setup, Advanced Setup, WAN, LAN, Routing, DSL, Print Server (highlighted), Port Mapping, IPsec, Certificate, Wireless, Diagnostics, and Management. The main content area is titled 'Print Server settings' and includes the text: 'This page allows you to enable / disable printer support.' Below this, there is a checkbox labeled 'Enable on-board print server.' which is checked. There are two text input fields: 'Printer name' with the value 'hp3845' and 'Make and model' with the value 'Hp DeskJet 3845'. A 'Save/Apply' button is located at the bottom right of the settings area.

**Step2:** Click on Add a printer from **Control Panel** of the **Win XP** computer and click "Next".

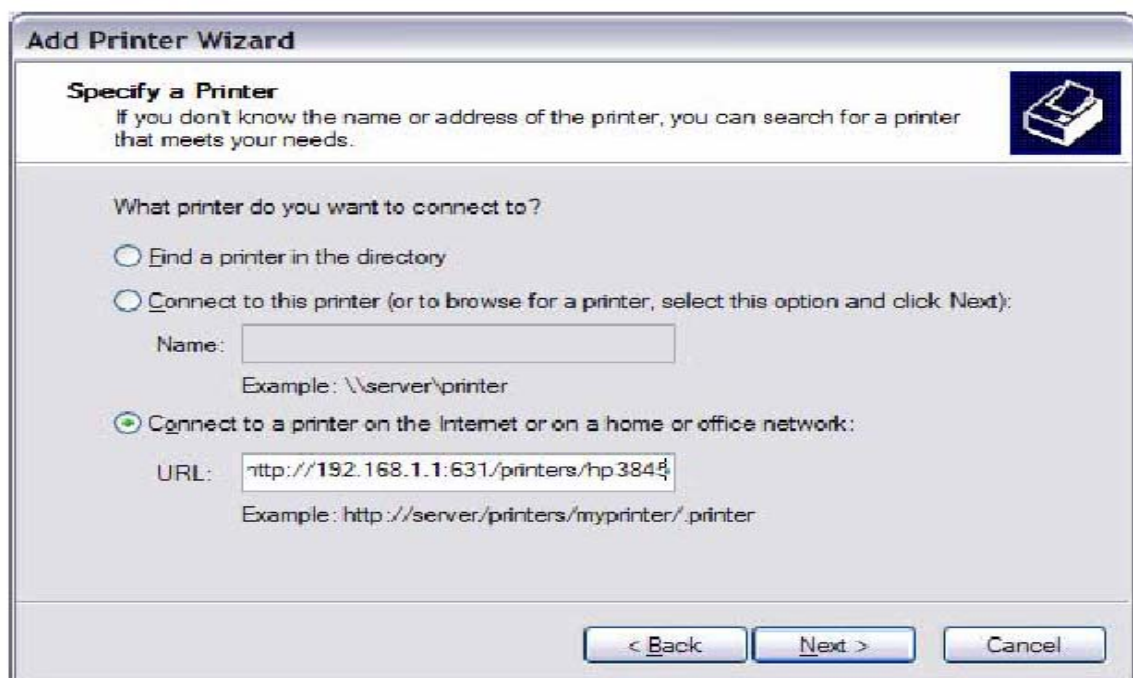


**Step3:** Select Network Printer and click "Next".

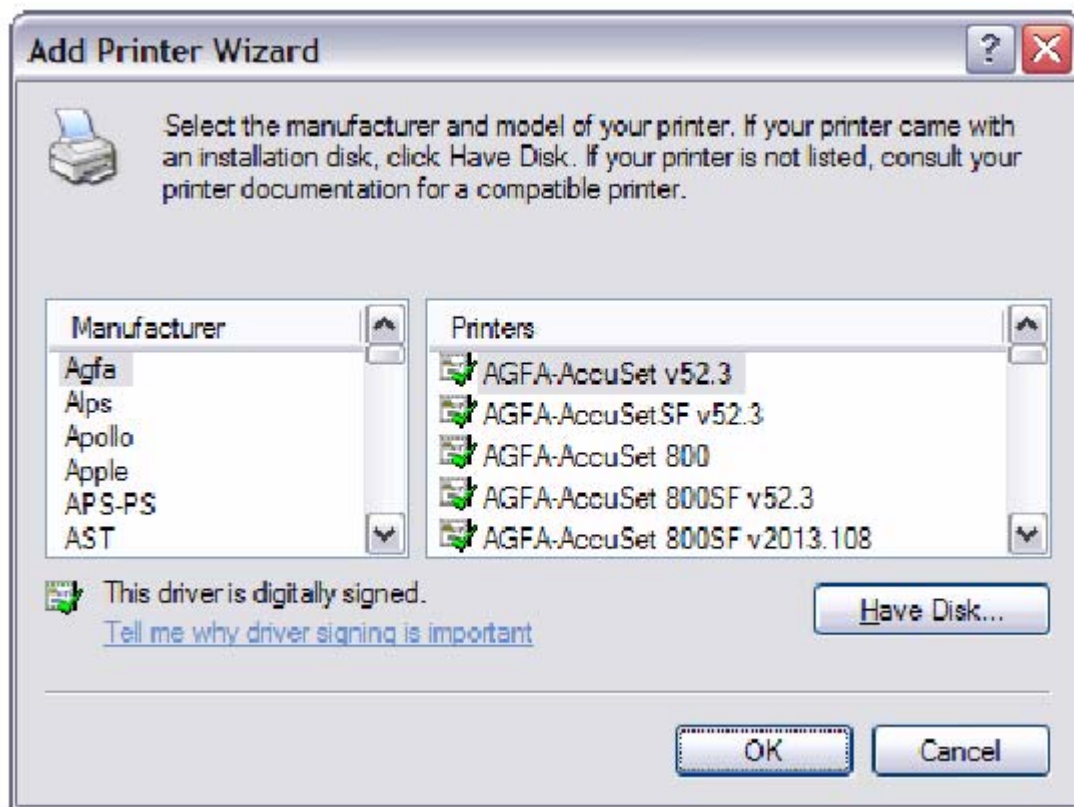


**Step4:** Select Connect to a printer on the Internet, type "<http://192.168.1.1:631/printers/hp3845>" and click "Next".

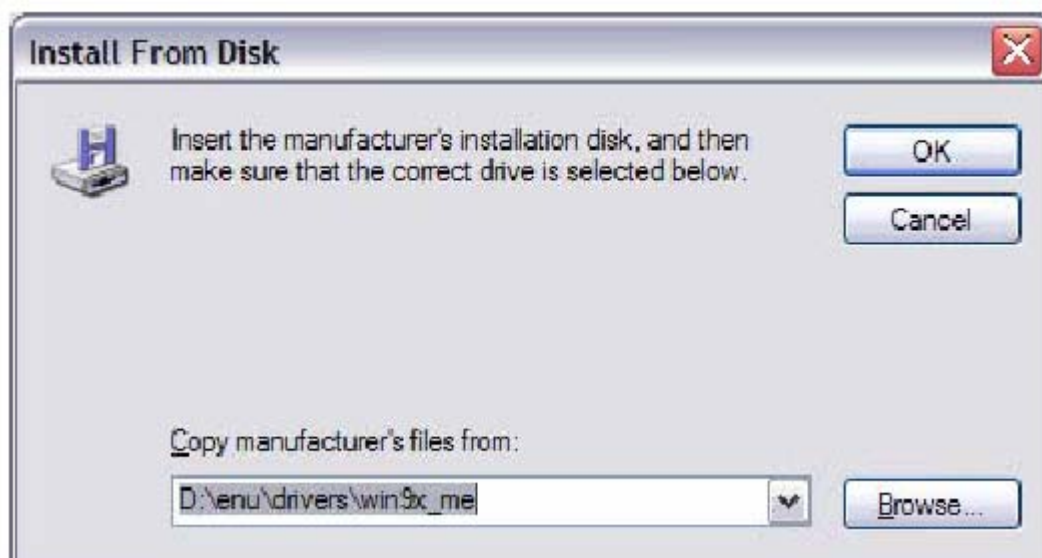
**The printer name "hp3845" must be the same name entered in the ADSL modem WEB UI "printer server setting" as in step 1.**



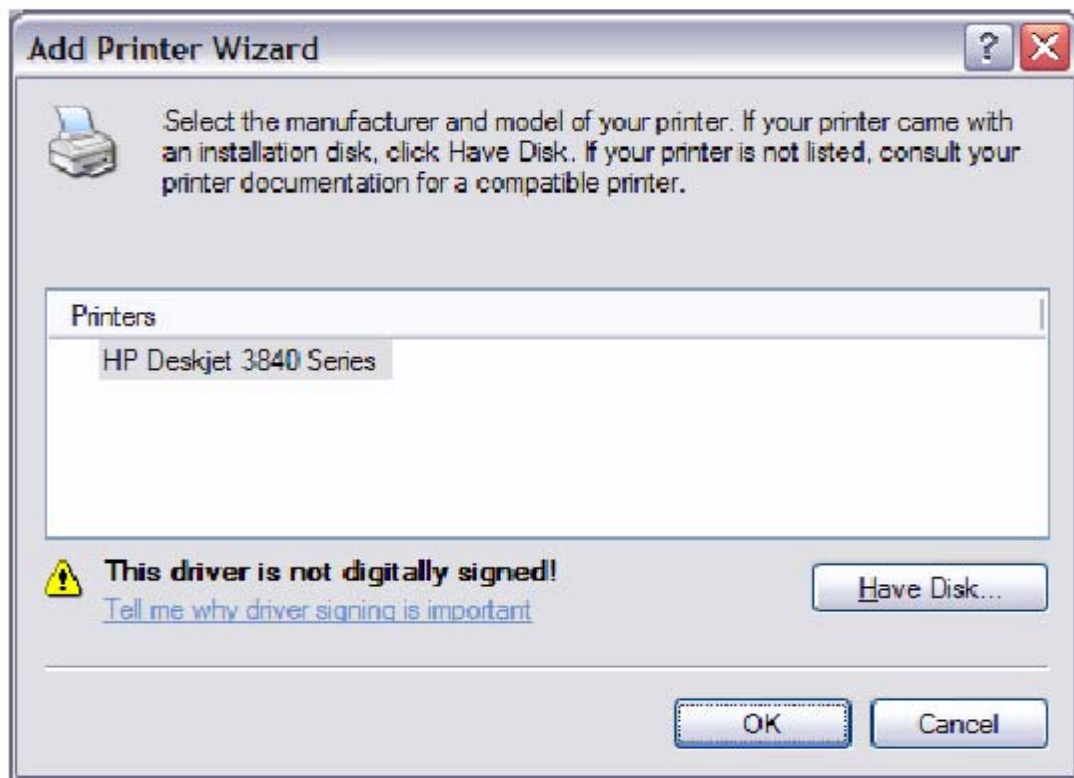
**Step 5:** Click "Have Disk", insert printer driver CD.



**Step 6:** Select driver file directory on CD-ROM and click "OK".



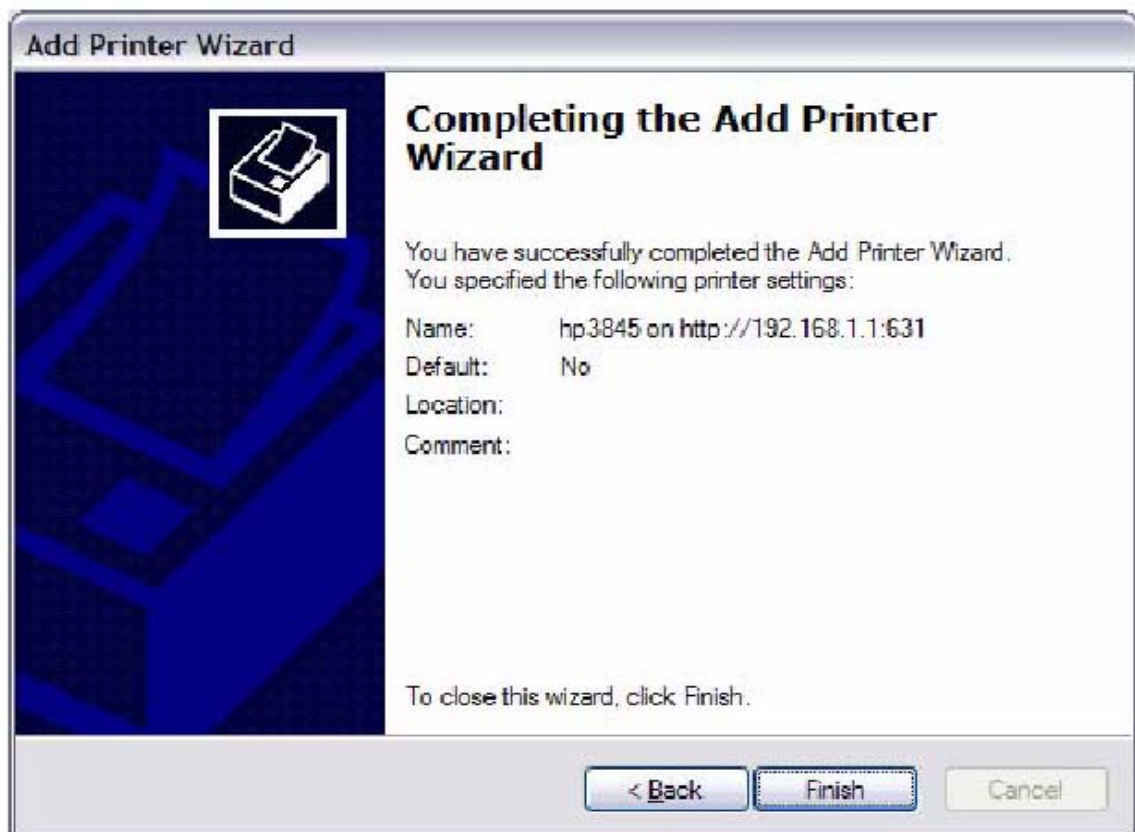
**Step 7:** Once the printer name appears, click "OK".



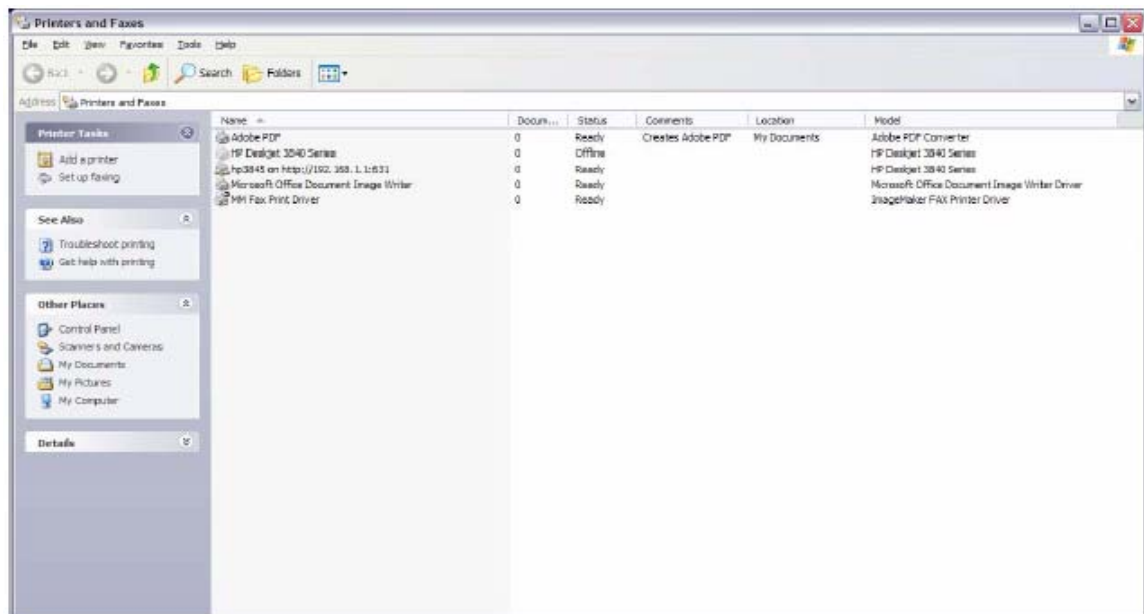
**Step 8:** Choose "Yes" or "No" for default printer setting and click "Next".



**Step 9:** Click "Finish".



**Step 10:** Check the status of printer from Windows Control Panel, printer window. Status should be shown ready.



## Appendix B: Firewall

### Stateful Packet Inspection

Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

### Denial of Service attack

Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the device can withstand are: ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack and Tear Drop.

### TCP/IP/Port/Interface filtering rules

These rules help in the filtering of traffic at the Network layer i.e. Layer 3.

When a Routing interface is created "Enable Firewall" must be checked.

Navigate to Advanced Setup -> Security -> IP Filtering, web page.

**Outgoing IP Filtering:** Helps in setting rules to DROP packets from the LAN interface. By default if Firewall is Enabled all IP traffic from LAN is allowed. By setting up one or more filters, particular packet types coming from the LAN can be dropped.

**Filter Name:** User defined Filter Name.

**Protocol:** Can take on any values from: TCP/UDP, TCP, UDP or ICMP

**Source IP Address/Source Subnet Mask:** Packets with the particular "Source IP Address/Source Subnet Mask" combination will be dropped.

**Source Port:** This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers(portX : portY) will be dropped.

**Destination IP Address/Destination Subnet Mask:** Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be dropped.

**Destination Port:** This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be dropped.

**Examples:**

1.    Filter Name                    : Out\_Filter1  
      Protocol                     : TCP  
      Source Address              : 192.168.1.45  
      Source Subnet Mask         : 255.255.255.0  
      Source Port                 : 80  
      Dest. Address               : NA  
      Dest. Sub. Mask            : NA  
      Dest. Port                  : NA

This filter will Drop all TCP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

2.    Filter Name                    : Out\_Filter2  
      Protocol                     : UDP  
      Source Address              : 192.168.1.45  
      Source Subnet Mask         : 255.255.255.0  
      Source Port                 : 5060:6060  
      Dest. Address               : 172.16.13.4  
      Dest. Sub. Mask            : 255.255.255.0  
      Dest. Port                  : 6060:7070

This filter will drop all UDP packets coming from LAN with IP Address/Sub.Mask 192.168.1.45/24 and a source port in the range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port in the range of 6060 to 7070.

**Incoming IP Filtering:**

Helps in setting rules to ACCEPT packets from the WAN interface. By default all incoming IP traffic from WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, particular packet types coming from the WAN can be Accepted.

**Filter Name:** User defined Filter Name.

**Protocol:** Can take on any values from: TCP/UDP, TCP, UDP or ICMP

**Source IP Address/Source Subnet Mask:** Packets with the particular "Source IP Address/Source Subnet Mask" combination will be accepted.

**Source Port:** This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

**Destination IP Address/Destination Subnet Mask:** Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be accepted.

**Destination Port:** This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

The WAN interface on which these rules apply needs to be selected by the user.

**Examples:**

1. Filter Name : In\_Filter1  
Protocol : TCP  
Source Address : 210.168.219.45  
Source Subnet Mask : 255.255.0.0  
Source Port : 80  
Dest. Address : NA  
Dest. Sub. Mask : NA  
Dest. Port : NA

Selected WAN interface: mer\_0\_35/nas\_0\_35

This filter will ACCEPT all TCP packets coming from WAN interface mer\_0\_35/nas\_0\_35 with IP Address/Sub. Mask 210.168.219.45/16 having a source port of 80 irrespective of the destination. All other incoming packets on this interface are DROPPED.

|    |                    |                  |
|----|--------------------|------------------|
| 2. | Filter Name        | : In_Filter2     |
|    | Protocol           | : UDP            |
|    | Source Address     | : 210.168.219.45 |
|    | Source Subnet Mask | : 255.255.0.0    |
|    | Source Port        | : 5060:6060      |
|    | Dest. Address      | :192.168.1.45    |
|    | Dest. Sub. Mask    | : 255.255.255.0  |
|    | Dest. Port         | : 6060:7070      |

This rule will ACCEPT all UDP packets coming from WAN interface mer\_0\_35/nas\_0\_35 with IP Address/Sub.Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

### **MAC Layer Filtering:**

These rules help in the filtering of traffic at the Layer 2. MAC Filtering is only effective on ATM PVCs configured in Bridge mode. After a Bridge mode PVC is created, navigate to Advanced Setup -> Security -> MAC Filtering web page.

### **Global Policy:**

When set to Forwarded the default filter behavior is to Forward all MAC layer frames except those explicitly stated in the rules. Setting it to Blocked changes the default filter behavior to Drop all MAC layer frames except those explicitly stated in the rules.

To setup a rule:

**Protocol Type:** Can be either PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP.

**Destination MAC Address:** Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular destination address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

**Source MAC Address:** Of the form, XX:XX:XX:XX:XX:XX. Frames with this particular source address will be Forwarded/Dropped depending on whether the Global Policy is Blocked/Forwarded.

**Frame Direction:**

LAN <=> WAN --> All Frames coming/going to/from LAN or to/from WAN.

WAN => LAN --> All Frames coming from WAN destined to LAN.

LAN => WAN --> All Frames coming from LAN destined to WAN

User needs to select the interface on which this rule is applied.

**Examples:**

1.

Global Policy: Forwarded

Protocol Type: PPPoE

Dest. MAC Addr: 00:12:34:56:78:90

Source MAC Addr: NA

Frame Direction: LAN => WAN

WAN Interface Selected: br\_0\_34/nas\_0\_34

Addition of this rule drops all PPPoE frames going from LAN-side to WAN-side with a Dest. MAC Addr. of 00:12:34:56:78:90 irrespective of its Source MAC Addr. on the br\_0\_34 WAN interface. All other frames on this interface are forwarded.

2.

Global Policy: Blocked

Protocol Type: PPPoE

Dest. MAC Addr: 00:12:34:56:78:90

Source MAC Addr: 00:34:12:78:90:56

Frame Direction: WAN => LAN

WAN Interface Selected: br\_0\_34/nas\_0\_34

Addition of this rule forwards all PPPoE frames going from WAN-side to LAN-side with a Dest. MAC Addr. of 00:12:34:56:78 and Source MAC Addr. of 00:34:12:78:90:56 on the br\_0\_34 WAN interface. All other frames on this interface are dropped.

### **Daytime Parental Control**

This feature restricts access of a selected LAN device to an outside Network through the router, as per chosen days of the week and the chosen times.

**User Name:** Name of the Filter.

**Browser's MAC Address:** Displays MAC address of the LAN device on which the browser is running.

**Other MAC Address:** If restrictions are to be applied to a device other than the one on which the browser is running, the MAC address of that LAN device is entered.

**Days of the Week:** Days of the week, when the restrictions are applied.

**Start Blocking Time:** The time when restrictions on the LAN device are put into effect.

**End Blocking Time:** The time when restrictions on the LAN device are lifted.

### **Example:**

User Name: FilterJohn

Browser's MAC Address: 00:25:46:78:63:21

Days of the Week: Mon, Wed, Fri

Start Blocking Time: 14:00

End Blocking Time: 18:00

When this rule i.e. FilterJohn is entered, a LAN device with MAC Address of 00:25:46:78:63:21 will be restricted access to the outside network on Mondays, Wednesdays and Fridays, from 2pm to 6pm. On all other days and time this device will have access to the outside Network.

## Appendix C: Pin Assignments

### Line port (RJ11)

| Pin | Definition | Pin | Definition |
|-----|------------|-----|------------|
| 1   | -          | 4   | ADSL_TIP   |
| 2   | -          | 5   | -          |
| 3   | ADSL_RING  | 6   | -          |

#### Pin Assignments of the RJ11 Port

### LAN Port (RJ45)

| Pin | Definition     | Pin | Definition    |
|-----|----------------|-----|---------------|
| 1   | Transmit data+ | 5   | NC            |
| 2   | Transmit data- | 6   | Receive data- |
| 3   | Receive data+  | 7   | NC            |
| 4   | NC             | 8   | NC            |

#### Pin assignments of the LAN Port



**Bridge Functions**

|                                   |             |
|-----------------------------------|-------------|
| Transparent bridging and learning | IEEE 802.1d |
| IGMP Proxy                        | Yes         |
| IGMP Snooping                     | Yes         |

**Routing Functions**

Static route, RIP v1 and RIP v2, NAT/PAT, DHCP Client/Server/Relay, DNS, ARP

**Security Functions**

|  |                              |
|--|------------------------------|
| Authentication protocols   | PAP, CHAP                    |
| VPN  | PPTP/L2TP/IpSec pass-through |
| Stateful Packet Inspection, Packet filtering, Denial Of Service protection, Traffic Conditioning, WFQ-based Bandwidth Management, HTTP proxy |                              |

**QoS**

L3 policy-based QoS, IP QoS, ToS

**Voice Functions**

|                     |                         |
|---------------------|-------------------------|
| SIP                 | RFC 3261                |
| Codec               | G.711, G.723.1, G.729ab |
| RTP                 | RFC 1889                |
| SDP                 | RFC 2327                |
| Caller ID           | ETSI based              |
| Life line           | Yes                     |
| Echo cancellation   | G.168                   |
| Silence suppression | Yes                     |

**Power**

|                        |                           |
|------------------------|---------------------------|
| External power adapter | 110-240Vac or 15dc / 1.6A |
|------------------------|---------------------------|

**Environmental Conditions**

|                       |                          |
|-----------------------|--------------------------|
| Operating temperature | 0 ~ 50 degrees Celsius   |
| Relative humidity     | 5 ~ 90% (non-condensing) |

**Dimensions**

205 mm (W) x 47 mm (H) x 145 mm (D)

**Note: Specifications are subject to change without notice**

## Appendix E: SSH Client

Linux OS comes with ssh client. Microsoft Windows does not have ssh client but there is a public domain one "putty" that you can download.

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

### **To access the IAD using Linux ssh client:**

From LAN: Use the IAD WEB UI to enable SSH access from LAN.

(default is enabled)

type: `ssh -l root 192.168.1.1`

From WAN: In the IAD, use WEB UI to enable SSH access from WAN.

type: `ssh -l support IAD-WAN-ip-address`

### **To access the IAD using Windows putty ssh client:**

From LAN: Use the IAD WEB UI to enable SSH access from LAN

(default is enabled)

type: `putty -ssh -l admin 192.168.1.1`

From WAN: In the IAD, use WEB UI to enable SSH access from WAN.

type: `putty -ssh -l support IAD-WAN-ip-address`